C.1 BACKGROUND

The United States Central Command (USCENTCOM), located at MacDill Air Force Base (AFB) in Florida, is one of the nine Department of Defense (DoD) unified combatant commands. USCENTCOM operates in theater for an Area of Responsibility (AOR) covering 20 nations in the Middle East, Central and South Asia, and the surrounding strategic waterways. The USCENTCOM mission is to direct and enable military operations and activities with allies and partners to increase regional security and stability in support of enduring United States (U.S.) interests.

The J6 Directorate (CCJ6) is responsible for management and oversight of USCENTCOM's Information Technology (IT) services to support the MacDill AFB Headquarters (HQ), CENTCOM Forward Headquarters (CFH) in Qatar, and the Security Cooperation Organizations (SCOs) throughout the AOR. The CCJ6 mission is to effectively and efficiently enable information sharing anytime, anywhere through a Joint and Combined Command, Control, Communications, and Computers (C4) Network-Centric Environment that is flexible, redundant, reliable, secure, and protected.

The Command, Control, Communications, and Computers Enterprise Support (C4ES) program provides CCJ6 with the enterprise IT support services necessary to support its mission.

C.2 SCOPE

The scope of this TO will support CCJ6 enterprise IT programs and assets at designated locations provided in section F.2. The scope of services include program management/project management, network operations and maintenance, telephony, cable and communications infrastructure, systems and server maintenance, helpdesk and desktop support, audio/visual and wireless technology, executive communications support, IT training, software and network engineering, defensive cyber operations, enterprise architecture, inventory management, knowledge management, and surge support. Travel is required within the Contiguous United States (CONUS) and to Outside the Contiguous United States (OCONUS) locations to support the requirements identified in this TO.

C.3 CURRENT INFORMATION TECHNOLOGY (IT)/NETWORK ENVIRONMENT

The following attachments have been provided for information on the current IT/Network environment:

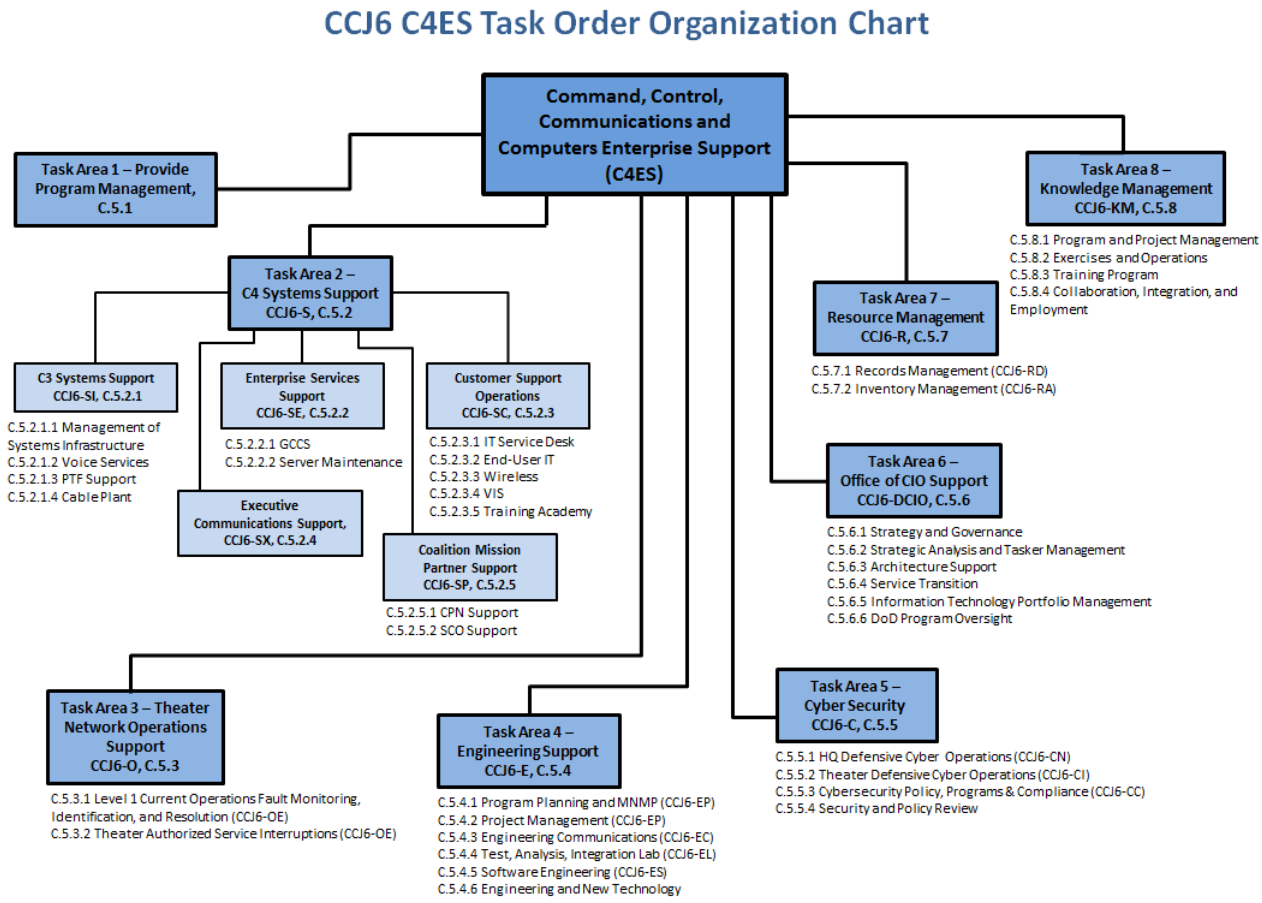
a. Section J, Attachment N – Regulations and Publications
b. Section J, Attachment P – Background and Sizing Information

C.4 OBJECTIVE

The objective of this TO is to support USCENTCOM in achieving full interoperability of its C4 systems and to gain efficiencies of scale that establish a world class network operation.

C.5 TASKS

The following is a depiction of the enterprise support tasks:



C.5.1 TASK AREA 1 – PROVIDE PROGRAM MANAGEMENT

The contractor shall provide program management support under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Performance Work Statement (PWS). The contractor shall identify a Program Manager (PM) by name who shall provide management, direction, administration, quality assurance, and leadership of the execution of this TO.

C.5.1.1 SUBTASK 1 – ACCOUNTING FOR CONTRACTOR MANPOWER REPORTING

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the USCENTCOM via a secure data collection site. The contractor is required to completely fill in all required data fields using the following web address: http://www.ecmra.mil/.

Reporting inputs will be for the labor executed during the period of performance during each Government Fiscal Year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the support desk at: http://www.ecmra.mil/.

Contractors may use Extensible Markup Language (XML) data transfer to the database server or fill in the fields on the website. The XML direct transfer is a format for transferring files from a contractor's systems to the secure web site without the need for separate data entries for each required data element at the website. The specific formats for the XML direct transfer may be downloaded from the web.

C.5.1.2 SUBTASK 2 – COORDINATE A PROJECT KICK-OFF MEETING

The contractor shall schedule and coordinate a Task Order Kick-Off Meeting within 10 workdays (Section F, Deliverable 1.1) following task order award at the location approved by the Government. The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include Key contractor Personnel, representatives from the directorates, other relevant Government personnel, and the Federal Systems Integration and Management Center (FEDSIM) Contracting Officer's Representative (COR).

At least three days prior to the Kick-Off Meeting, the contractor shall provide a Kick-Off Meeting Agenda for review and approval by the FEDSIM COR and the TPOC prior to finalizing. The agenda shall include, at a minimum, the following topics/deliverables:

a. Points of contact (POCs) for all parties
b. Personnel discussion (i.e., roles and responsibilities and lines of communication between contractor and Government)
c. Staffing Plan and status
d. Updated Draft Transition-In Plan (Section F, Deliverable 1.10) (Government comments shall be incorporated into the Final Transition-In Plan)
e. Security discussion and requirements (i.e., building access, badges, Common Access Cards (CACs))
f. Invoicing considerations
g. Transition discussion

The Government will provide the contractor with the number of Government participants for the Kick-Off Meeting and the contractor shall provide sufficient copies of the presentation for all present.

The contractor shall draft and provide a Kick-Off Meeting minutes (Section F, Deliverable 1.13) report documenting the Kick-Off Meeting discussion and capturing any action items.

C.5.1.3 SUBTASK 3 – PREPARE A MONTHLY STATUS REPORT (MSR)

The contractor PM shall develop and provide an MSR (Section J, Attachment F) (Section F, Deliverable 1.2). The MSR template is a suggested format; however the contractor may modify the format upon TPOC and/or COR approval, and tailor to its communication preferences. The MSR shall include the following:

a. Activities during reporting period, by task (include: on-going activities, new activities, activities completed; progress to date on all above mentioned activities). Start each section with a brief description of the task.
b. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
c. Personnel gains, losses, and status (security clearance, etc.).
d. Government actions required.
e. Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
f. Summary of trips taken, conferences attended, etc. (attach Trip Reports to the MSR for reporting period).
g. Accumulated invoiced cost for each CLIN up to the previous month. This shall also include any outstanding incurred costs from pending invoices.
h. Projected cost of each CLIN for the current month.

C.5.1.4 SUBTASK 4 – CONVENE TECHNICAL STATUS MEETINGS

The contractor PM shall convene a monthly Technical Status Meeting with the TPOC, FEDSIM COR, and other Government stakeholders (Section F, Deliverable 1.14). The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The contractor PM shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the FEDSIM COR within five workdays following the meeting (Section F, Deliverable 1.15).

C.5.1.5 SUBTASK 5 – PREPARE A PROJECT MANAGEMENT PLAN (PMP)

The contractor shall document all support requirements in a PMP. The contractor shall provide the Government with a draft PMP (Section F, Deliverable 1.3) on which the Government will make comments. The final PMP (Section F, Deliverable 1.4) shall incorporate the Government's comments.

The PMP shall:

a. Describe the proposed management approach.
b. Contain detailed Standard Operating Procedures (SOPs) for all tasks.
c. Include milestones, tasks, and subtasks required in this TO.
d. Provide for an overall Work Breakdown Structure (WBS) with a minimum of three levels and associated responsibilities and partnerships between Government organizations.

e. Describe in detail the contractor's approach to risk management under this TO.
f. Describe in detail the contractor's approach to communications, including processes, procedures, communication approach, and other rules of engagement between the contractor and the Government.
g. Include milestones, tasks, and subtasks required in this TO.
h. Include the contractor's Baseline Quality Control Plan (QCP).

C.5.1.6 SUBTASK 6 – UPDATE THE PROJECT MANAGEMENT PLAN (PMP)

The PMP is an evolutionary document that shall be updated annually at a minimum (Section F, Deliverable 1.5). The contractor shall work from the latest Government-approved version of the PMP.

C.5.1.7 SUBTASK 7 – PREPARE TRIP REPORTS

The Government will identify the need for a Trip Report when the request for travel is submitted (Section F, Deliverable 1.6). The contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, and point of contact (POC) at travel location. Trip reports shall also contain Government approval authority, total cost of the trip, a detailed description of the purpose of the trip, and any knowledge gained. At a minimum, trip reports shall be prepared with the information provided in Section J, Attachment G.

C.5.1.8 SUBTASK 8 – UPDATE BASELINE QUALITY CONTROL PLAN (QCP)

The contractor shall update the QCP submitted with its proposal and provide a final baseline QCP as required in Section F (Section F, Deliverable 1.7). The contractor shall periodically update the QCP, as required in Section F (Section F, Deliverable 1.8), as changes in program processes are identified.

Within the QCP, the contractor shall identify its approach for providing quality control in meeting the requirements of the TO. The contractor's QCP shall describe its quality control methodology for accomplishing TO performance expectations and objectives. The contractor shall fully discuss its validated processes and procedures that provide high quality performance for each Task Area. The QCP shall describe how the processes integrate with the Government's requirements.

C.5.1.9 SUBTASK 9 – STAFFING MATRIX

The contractor shall develop and update a staffing matrix (Section F, Deliverable 1.9) to show arriving, departing, and transfers of contractor personnel on the TO. The matrix shall include, at a minimum: task numbers, job descriptions, names, security clearance levels, arrival and departure dates, and company names.

C.5.1.10 SUBTASK 10 – TRANSITION-IN

The contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during and after transition. All transition activities shall be completed 60 calendar days after TO start date. The updated Draft Transition-In plan shall be

presented at the kick-off meeting (Section F, Deliverable 1.10) and submitted for final approval within three days following the kick-off meeting (Section F, Deliverable 1.11).

C.5.1.11 SUBTASK 11 – TRANSITION-OUT

The contractor shall provide Transition-Out support when required by the Government. The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to an incoming contractor/Government personnel at the expiration of the TO. The contractor shall provide a draft Transition-Out Plan within six months of Project Start (PS) (Section F, Deliverable 1.12). The Government will work with the contractor to finalize the Transition-Out Plan in accordance with Section E. At a minimum, this Plan shall be reviewed and updated on an annual basis. Additionally, the Transition-Out Plan shall be reviewed and updated quarterly during the final Option Period or Award Term (Section F, Deliverable 1.16).

In the Transition-Out Plan, the contractor shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

a. Project management processes
b. Points of contact
c. Location of technical and project management documentation
d. Status of ongoing technical initiatives
e. Appropriate contractor to contractor coordination to ensure a seamless transition
f. Transition of Key Personnel
g. Schedules and milestones
h. Actions required of the Government

The contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings or as often as necessary to ensure a seamless transition-out.

The contractor shall begin implementing its Transition-Out Plan no later than (NLT) 90 calendar days prior to expiration of the TO.

C.5.1.12 SUBTASK 12 – PERFORMANCE SCORECARD

The contractor shall maintain and enhance the C4ES Scorecard Application (C4ES SA) located on Secret Internet Protocol Router Network (SIPRNet). The C4ES SA is used to collect task area performance results for the USCENTCOM C4ES program. The data gathered in the scorecards will be compiled to populate a series of dashboards at the task area, division and program levels on a monthly basis. The C4ES SA shall be used by contractor program management, task area leads and task managers and Government performance monitors.

The C4ES SA shall maintain the following capabilities:

a. A Training section offering access to new users to learn about the application and how to report and evaluate performance.
b. Individual Scorecards for each task that include summaries of metrics, supporting documents, areas for Task Area Leads, Task Managers and Government Performance

Monitors to provide input on contractor accomplishments and/or areas for improvement as well as an subjective evaluation section for scoring.

c. An archived section offering access to previous months' scorecards.
d. Sections describing each metric used on the TO.
e. A settings section to allow for user or role changes and assignments of backups
f. A Frequently Asked Questions (FAQ) and Help section.

C.5.2 TASK AREA 2 – C4 SYSTEMS SUPPORT (CCJ6-S)

The contractor shall provide C3 Systems Support, Enterprise Services Support, Customer Support Operations (CSO), Executive Communications Support, Training Academy, and Coalition Mission Partner Support. In support of the tasks/subtasks, the contractor shall perform the following technical, management and operations functions:

a. Perform tasks in accordance with applicable HQ USCENTCOM and Theater policies, regulations, regulations guidelines and Memorandums of Agreement (MOAs).
b. Develop an overall Concept of Operations (CONOPS) (Section F, Deliverable 2.1) and maintain the CONOPS throughout the period of performance.
c. Provide recommendations on researched and tested technologies showing potential cost savings using applications/hardware or process improvements that show efficiencies in completing tasks covered in this TOR (Section F, Deliverable 2.2).
d. Ensure all scheduled and unscheduled service outages are identified and coordinated throughout USCENTCOM. Authorized scheduled outages shall be performed at a time that cause the least mission impact and inconvenience to users.
e. Maintain 100 percent accountability of all assets within the scope of this task area. Track and provide budgeting, forecasting, and consumption rate information in order to best utilize and manage spare equipment and ensure all necessary repair parts are available to quickly return assets to operational status. Provide a report on all assets as requested by the Government (Section F, Deliverable 2.3).
f. Perform, schedule, and document Preventive Maintenance Inspections (PMI) on the systems, devices, and associated hardware within the scope of this task in accordance with (IAW) manufacturer's manuals and/or vendor best practice recommendations. Maintain PMI completion documents on file for review by USCENTCOM upon request (Section F, Deliverable 2.4). The contractor shall create and maintain a schedule to perform preventive maintenance IAW the equipment manufacturer's manuals and USCENTCOM direction (Section F, Deliverable 2.5). PMIs shall be annotated in the schedule. Provide preventive, remedial, and corrective maintenance to ensure all on-line and spare equipment, to include spare equipment strings, is in proper and full operating condition as described by the equipment manufacturer and applicable Defense Information Systems Agency (DISA) circulars without degradation of service. All equipment, regardless of whether or not it is providing service at any particular time, shall be maintained in fully operational condition.
g. The contractor shall investigate, troubleshoot, and repair information exchange issues (i.e., email, web sites, portals, file transfers) between the USCENTCOM IT enterprise

and those of other organizations who support USCENTCOM missions, to include Department of State and foreign military organizations.

h. Monitor USCENTCOM's IT Service Management queues in order to take the appropriate action to expedite processing and resolve customer-related incidents, changes, and problems.

i. Maintain 100 percent accountability of all communications security (COMSEC) items IAW National Security Agency (NSA)/DoD/USCENTCOM COMSEC policies, guidelines, and procedures.

j. Recommend a prioritized service restoration list for returning systems and services to operation in the event of a catastrophic failure, to include restoring station lines, systems, devices, and cabling (Section F, Deliverable 2.6). The identity and location of circuits may vary over the life of the TO and will be provided by USCENTCOM. The list shall be prioritized by each network and system/device operated and maintained by the contractor. The list shall also include information on customer types, priorities, locations, and any spare parts/equipment requirements. The list shall be updated as changes occur either to the system architecture or to the supported customers. The list shall be published on a quarterly basis.

k. Coordinate with Configuration Management to ensure that any new or updated records for configuration items within the scope of this task area are entered in the Configuration Management Database (CMDB) IAW USCENTCOM standards.

l. Update/generate documentation and artifacts required to support inspections for any network/system within the scope of this task, including security accreditation documentation for all systems/networks (Section F, Deliverable 2.7).

m. Conduct trend analysis of common problems and system performance, change requests, average device and service uptime, service outage durations and frequencies, incident status updates, analyses of training effectiveness, statistics on courses conducted and other parameters identified as necessary to best report on the state of the USCENTCOM enterprise.

n. Review, edit, and maintain diagrams within 30 calendar days after TO award IAW USCENTCOM regulations, policies, and standards (Section F, Deliverable 2.8). Maintain newly developed and existing diagrams and synchronize any modifications IAW DoD Information Assurance Certification and Accreditation Process (DIACAP) and/or Risk Management Framework (RMF) standards. Updates to these physical and logical diagrams of systems, networks, infrastructure, and storage shall be completed within 24 hours after any changes have been implemented. Validated versions of these physical diagrams shall be published in the standardized format specified by USCENTCOM and agreed to by the contractor at least on a monthly basis.

o. Maintain a continuity folder of documentation pertaining to all systems and technologies that are relevant to this task area in order to facilitate training (Section F, Deliverable 2.9). As new systems and technologies are introduced, develop and maintain additional required information.

p. Develop and publish consolidated folder of lessons learned during troubleshooting, covering best practices, Tactics, Techniques, and Procedures (TTPs), policies and

procedures on all aspects of the systems environment related to this task area (Section F, Deliverable 2.10).

q. After all major system/network outages affecting systems/networks within the scope of this task, analyze the factors contributing to the outage, as well as the effectiveness of actions taken to restore services. The contractor shall publish these analyses and findings in an After Action Report (AAR) no later than the close of business on the next duty day after restoring the system/network to operational status (Section F, Deliverable 2.11).

r. Respond to outages, degradations, and hazardous condition (HAZCON) events for all networks and systems within the scope of this sub-task area IAW USCENTCOM policies, regulations, and procedures.

s. Detect and compile information on recurring problems to determine the effectiveness of corrective actions taken to resolve problems. Recurring problems shall be tracked by service (e.g., printing, e-mail, phone, etc.). Analyze the compiled information to identify situations where problem resolution does not provide a stable fix for an issue and suggest Courses of Actions (COAs) for improving results. Implement COAs selected and monitor their impact on performance to verify that the frequency of recurring incidents is being reduced. Utilize trend analysis methods and other means to visualize the data.

t. Develop and maintain detailed operational checklists (Section F, Deliverable 2.12) to ensure all contractor personnel follow standard tactics, techniques, and procedures (TTPs) when preparing for, executing, and validating results of any tasks, processes, authorized service interruptions (ASIs), or maintenance actions impacting services and systems within the scope of this task area. Develop checklist(s) for each task/process identified and ensure contractor personnel are properly trained to perform the daily operational tasks using the applicable checklist(s). The checklists and associated TTPs shall be made available for review by USCENTCOM.

u. Package, transport, and ship equipment to and from USCENTCOM-supported locations and buildings IAW USCENTCOM logistical support policies, regulations, guidelines, and procedures.

v. Participate in reviews of new systems or modifications of existing systems.

w. Report any temporary changes made to systems and services within the scope of this area within 30 minutes. If the change has the potential for a significant impact, the change shall be coordinated within USCENTCOM prior to implementation.

x. Coordinate internally with other Technical Support Teams and externally with third parties and vendors to troubleshoot outages, service degradations, and HAZCON events and to document fix actions taken to resolve these issues.

y. Install software patches, new releases, and Information Assurance (IA) updates to ensure all systems and devices within the scope of this task are compliant with applicable Security Technical Information Guides (STIGs) and Security Directives. Ensure all IA updates are applied within required deadlines.

z. Collect information needed to develop management reports that provide metrics and trend analyses of common problems.

aa. Perform site surveys, determine COAs, develop drawings, provide cost and time estimates, generate assembled material lists, and create documentation in support of

systems installations and systems infrastructure installations (Section F, Deliverable 2.13).

bb. Manage, maintain, and post a daily Master Station Log (MSL) and shift change procedures for all tasks to ensure proper information flow across shifts (Section F, Deliverable 2.14). This MSL shall provide a record of all maintenance requirements, functions, and corrective actions taken. The contractor shall document when the deficient function and/or operation was first discovered/reported, as well as the exact time it was corrected and when the service, function, and/or operation was restored.

cc. Provide situational awareness to Watch Officers on all activity associated with USCENTCOM systems and services.

dd. Provide focal point communications for all J6 and applicable J2 (Intelligence Directorate) outages and issues on all networks / services.

ee. Provide knowledge transfer to pertinent U.S. Government personnel on existing and future implemented technologies/systems when transitioning task responsibilities.

ff. Assist Inventory Management in Task 5.7.2 as required.

gg. The contractor shall develop and maintain a Disaster Recovery Plan (Section F, Deliverable 2.43) for Continuity of Operations (COOP). The plan shall designate a list of Contractor personnel as a Disaster Recovery Team and identify any associated recall information. The plan shall address a process to assess damage to systems/networks within the scope of this TO and recommend Courses of Action (COAs) to USCENTCOM to mitigate damage and expedite system/network restoral.

hh. In the event of a real-world disaster, the contractor shall implement the Disaster Recovery Plan and recommended COAs (with Government approval) in order to restore systems and networks to operational status. The Contractor shall utilize pre-designated Disaster Recovery Teams to provide on-site operations at MacDill AFB, until the USCENTCOM Commander orders an evacuation, at the CONUS Communications Restoral Site and at CENTCOM Forward Headquarters.

C.5.2.1 SUBTASK 1 – C3 SYSTEMS SUPPORT (CCJ6-SI)

The contractor shall provide the following support for all of the tasks/subtasks under the Command, Control, and Communications (C3) System Support sub-Task Area:

a. Participate in training activities, exercises, and real world deployments.

b. Provide deployable Continuity of Operations (COOP) communications capabilities during emergency situations (e.g. hurricanes, fire, flood, cable cuts, power outages, equipment failures, etc.). In the event of a real-world emergency, COOP support could be required for extended periods of time.

c. Prepare and update accreditation packages and maintain accreditation documentation folders for new or existing systems and equipment (Section F, Deliverable 2.15).

C.5.2.1.1 MANAGEMENT OF SYSTEMS INFRASTRUCTURE

As part of managing the HQ Systems Infrastructure, the contractor shall provide the Operations and Maintenance (O&M) of the USCENTCOM Network Infrastructure. This infrastructure

includes multiple, disparate Tier 1 and Tier 2 network architectures. The contractor shall operate, monitor, manage, maintain, install, and troubleshoot USCENTCOM network infrastructure devices and services within the scope of this task. The contractor shall support all aspects of network infrastructure management including policies, procedures, implementation, technology integration, virtual encryption and guidance for both scheduled and unscheduled maintenance. HQ Systems Infrastructure provides support to HQ USCENTCOM, CFH with secondary sites within the Tampa Bay metropolitan area, other Continental United States (CONUS) locations, supported embassy networks, and other locations within USCENTCOM's AOR. Travel may be required to support service requests through Temporary Duty (TDY) requests.

The contractor shall:

a. Maintain and enhance a comprehensive Network Infrastructure (NI) Maintenance Program for all networks, systems, and services within the scope of this task to include wireless access points, controllers and associated equipment.
b. Maintain the SOPs for testing and validating the operational status of network infrastructure systems and services.
c. Provide on-site support for all systems/services/networks operated and maintained within the task scope.
d. Provide situational awareness on HQ systems infrastructure to the USCENTCOM Joint Cyberspace Communications Center (JCCC) via a designated liaison.
e. Baseline and maintain all device configurations (to include software) utilizing Information Assurance (IA) STIGs and maintain configuration/compliance control and policy management of all network devices within the scope of this task.
f. Manage the HQ USCENTCOM Internet Protocol (IP) addressing space for all supported networks and all directly supported sites.
g. Operate and maintain the USCENTCOM Dynamic Host Configuration Protocol (DHCP) services for all supported networks.
h. Maintain graphical representation models of the logical CENTCOM HQ Enterprise Networks, as required, to provide CENTCOM's Tier 2 monitoring tools suite a complete high-level overview of network performance and health reporting statistics of network infrastructure devices (Section F, Deliverable 2.16).
i. Deploy and maintain appropriate network device configurations to support the CENTCOM Enterprise network monitoring suite of tools for Tier 2 (e.g., Simple Network Management Protocol (SNMP) Profiles, Access Control List (ACL) Configurations and Trap Destinations).
j. Provide documentation during non-duty hours of network impacting events (i.e. Master Station Log) (Section F, Deliverable 2.14).
k. Designated technical lead shall carry the USCENTCOM-issued communication device during duty hours to respond to critical requests.
l. Provide in-depth weekly status updates to include, but not limited to; current lines of effort, status of projects and Information Technology Service Management (ITSM) (currently Remedy) tickets to designated CCJ6-SI Government personnel (Section F, Deliverable 2.17).

C.5.2.1.1.1 COMMERCIAL SOLUTIONS FOR CLASSIFIED (CSfC) SUPPORT

Commercial Solutions for Classified (CSfC) is responsible for designing, implementing, operating, and maintaining a mobile access (MA) capability package (CP) for the HQ USCENTCOM campus, CFH, homes, quarters, and support end user devices (EUDs) deployed worldwide. CSfC Access points are located throughout HQ USCENTCOM and CFH campuses and support unclassified and classified wireless networks. The contractor is required to comply with policies of the NSA's Information Assurance Directorate (IAD) Commercial Solutions for Classified Program (CSfC) in support of this task.

The Contractor shall:

a. Provide O&M support for CSfC infrastructure devices (e.g. routers, domain controllers, certificate servers, wireless controllers, VPN devices, firewalls, etc.).
b. Provide 24x7 security administration for the Inner Encryption Endpoints and supporting components on Enterprise (Red) networks and Gray networks. Security Administrator(s) shall be different individuals from the Security Administrator(s) for the Outer VPN Gateway and supporting components on Gray networks.
c. Ensure that the latest security software patches and updates (such as IAVAs) are applied to each CSfC device.
d. Document and report security-related incidents to the appropriate authorities.
e. Coordinate and support product logistic support activities including integration and maintenance.
f. Employ adequate defenses of auxiliary mobile access (MA) network devices.
g. Ensure that the MA solution remains compliant with the latest version of the NSA's capability package (CP).
h. Provision and maintain end user devices (EUDs) and EUD certificates in accordance with the CP.
i. Maintain, monitor, and control all security functions for the certificate authority (CA).
j. Administer the CA, including authentication of all components requesting certificates.
k. Maintain and update the certificate revocation list (CRL).
l. Review, manage, control, and maintain security audit log data.
m. Document and report security-related incidents to the appropriate authorities.
n. Process and respond to CSfC alerts from the NSA.
o. Document, maintain, and test the MA solution IAW the CP.
p. Respond and resolve incidents affecting the MA solution.

C.5.2.1.2 VOICE SERVICES

The contractor shall provide maintenance for all of USCENTCOM's telephony services and associated directorate sub-accounts. USCENTCOM telephony equipment and technology include but are not limited to the following:

a. Voice Over Internet Protocol (VoIP) phones

b. Voice Over Secure Internet Protocol (VoSIP) phones, to include video / voice instruments.
c. Avaya/Nortel/NEC Time Division Multiplexing (TDM) and VOIP telephony switching systems servicing USCENTCOM HQ's
d. Secure Telephone Equipment (STEs)
e. Cisco Unified Communications Managers supporting multiple networks
f. Cisco Unity Connection/Nortel/Avaya Voicemail servers
g. Cisco Meeting Place Conferencing and Audio Servers
h. Avaya Automatic Call Distribution (ACD) system servers

The contractor shall maintain property accountability for all phone systems and equipment listed above. The contractor shall be responsible for the preparation, configuration, testing, training, issuance, and receipt of STE, OMNI, TDM, and VoIP/VoSIP devices. This includes activities such as troubleshooting and performing minor repairs on STEs, OMNIs, TDM and VoIP/VoSIP phones. The contractor shall establish and maintain asset inventory management of all telephony devices, STEs, and OMNIs. The contractor is also responsible for monitoring the usage of telephony services to include the review/audit/reconciliation of usage logs. Additionally, the contractor shall coordinate the installation of TDM and VoIP/VoSIP telephones.

The contractor shall operate, monitor, maintain, install, and troubleshoot USCENTCOM telephony devices and services at designated sites located at and around HQ USCENTCOM, CFH, embassies, and locations within USCENTCOM's AOR. CONUS and OCONUS travel may be required at remote locations (no personnel are permanently located).

The contractor shall perform the following on-site support IAW USCENTCOM policies, regulations, and guidance and in locations specified within the scope of this task:

a. Provide on-site coverage for all systems/services operated and maintained by the Voice Services Technical Support Team. On-call support shall be provided during non-duty hours. The maximum time for reporting to duty station after on-call support is requested is one hour from the time of notification. A comprehensive on-call/alert roster shall be maintained and updated on a monthly basis.
b. Provide desk side and outside plant support to USCENTCOM users.
c. Provide a Tier 2 O&M support mechanism for the CM-6 telephone systems currently maintained by the US Air Force 6th Communications Squadron (CS). Tier 2 O&M support for the CM-6 telephone system includes voicemail and ACD systems. Unresolved issues will be escalated to the contractor from the 6th CS. The contractor shall restore and resolve all telephony issues.
d. Install/maintain/remove telephony services in the quarters of other USCENTCOM General Officers (GO)/Flag Officers (FO).
e. Install, configure, and maintain USCENTCOM VoIP and VoSIP Call Managers at all support locations.
f. Install, configure, and maintain TDM, VoIP, and VoSIP devices IAW USCENTCOM policies, regulations, and procedures.

g. Maintain USCENTCOM telephone accounts and associated directorate sub-accounts pertaining to VoIP, VoSIP, OMNI, and STE devices. The contractor shall troubleshoot issues with these devices as necessary.
h. Monitor voice circuits and devices to facilitate the early detection of incidents, impending outages, or degradations.
i. Verify and update the Telephone Subscriber Database to include, but not limited to, numbers, subscribers, and port assignments (Section F, Deliverable 2.18).
j. Perform Annual Telecommunications and Monitoring Assessment Program (TMAP) inspections. Publish TMAP reports documenting findings and recommendations annually (Section F, Deliverable 2.19).

C.5.2.1.3 PATCH AND TEST FACILITY (PTF) SUPPORT

The PTF is the primary service delivery point at HQ USCENTCOM for fixed long-haul communication infrastructure services. PTF contractors support USCENTCOM communication requirements and C4 initiatives. PTF team members are responsible for restoring services in accordance with local and higher level policy. The contractor shall operate and maintain USCENTCOM fixed and deployable IT systems to include transmission systems, hardware, and software associated with long-haul communications systems and tactical network infrastructure equipment.

The contractor shall perform PTF in accordance with Defense Information Systems Agency Circular (DISAC) 310-70-1. The contractor shall also manage a COMSEC sub-account that will provide COMSEC support and COMSEC re-key to all of J6 communication circuits as well as COMSEC key updates for communications circuits. PTF provides support to HQ USCENTCOM, CFH, and other supported locations including multiple sites on MacDill AFB and within the Tampa Bay metropolitan area, other CONUS locations, locations within USCENTCOM's AOR and other supported Combatant Command (COCOM) AORs. Travel may be required to support service requests (CONUS and OCONUS) through TDY requests.

The contractor shall:

a. Provide on-site technical support for all circuits/systems/services operated and maintained by the PTF Technical Support Team.
b. Provide expertise and advice on PTF to the USCENTCOM JCCC via a designated liaison.
c. Ensure all scheduled authorized outages for circuits, station lines, systems, and devices within the scope of this task are identified, coordinated, and reported IAW USCENTCOM policies, regulations, and guidelines and DISAC 310-70-1.
d. Document all outages that directly affect General Officer/Flag Officer (GO/FO) communications in the Incident Management System regardless of length of the outage.
e. Acknowledge the outage and open a trouble ticket within timelines established in DISA circulars once notified of an outage by USCENTCOM, DISA, or other pertinent agency.
f. Open a new record for outages that originate outside of USCENTCOM or affected users that are unable to record an outage in the Incident Management System and cannot be resolved after ten minutes.

g. Complete a circuit history folder review for all circuits traversing the PTF on an annual basis.

h. Manage, maintain, and post a daily MSL IAW DISAC 310-70-1 and shift change procedures to ensure proper information flow across shifts (Section F, Deliverable 2.14). In addition to the MSL, the contractor shall provide a Daily Systems/Circuit Status Report that will be provided to Government leadership prior to the morning stand up meeting (Section F, Deliverable 2.20).

i. Monitor circuits and networks within the scope of this task to assess their health and to facilitate early detection of incidents, impending outages, or degradations. On an hourly basis, walk through and thoroughly inspect all USCENTCOM PTFs, and any other facilities, to ensure all equipment is operating correctly, including environmental systems. Any deficiencies noted during the inspection shall be annotated on the MSL. Corrective action shall be taken / requested and the incident shall be tracked until system outages and/or facility deficiencies are repaired or corrected.

j. Determine the methodology for restoration of communication services to include moderate equipment configuration changes or modifications within the PTF. The contractor shall maintain connection services between the user and Wide Area Network (WAN) equipment. Local connectivity may include fiber optic/copper cabling, connectors, and other ancillary devices (e.g., line drivers, modems, Channel Service Units (CSUs)/Data Service Units (DSUs), and IP devices (e.g., routers, switches, firewalls and encryption devices)) required to provide end user services.

k. Troubleshoot and repair interfaces on technical control equipment to include, but not limited to, the following interfaces: RS-449/422, RS-530, RS-232, and Conditioned Diphase (CDI), Synchronous Digital Hierarchy (SDH), and Ethernet.

l. Provide fault isolation and restoration of strategic, base, and tactical communications circuits/systems to include, but not limited to, voice, video, data, radio, fiber optic, satellite, and command and control information networks.

m. Identify, troubleshoot, and resolve C4 compatibility issues between deployed tactical assets and fixed components.

n. Program, load, maintain, and account for all cryptographic equipment within the scope of this task in accordance with applicable Air Force, DoD, and U.S. Government guidance.

o. Complete daily, weekly, monthly, quarterly, and yearly cryptologic changeovers and updates IAW USCENTCOM policies, regulations, and guidelines.

p. Provide a qualified COMSEC Responsible Officer (CRO) and alternate. This CRO shall manage all COMSEC material and keys assigned to the sub-account, prepare for command and Major Command (MAJCOM) inspections, account for COMSEC documents, and conduct training for all personnel with authorized access.

C.5.2.1.4 CABLE PLANT SUPPORT

The contractor shall provide the engineering, installation, testing, and maintenance of the secure/non-secure voice, video, data, and radio frequency cable infrastructure. Support is required for HQ USCENTCOM, multiple locations on MacDill AFB, sites within the Tampa Bay metropolitan area, other CONUS locations, CFH, and locations within USCENTCOM's

AOR. Travel may be required to support service requests (CONUS and OCONUS) through TDY requests.

The contractor shall perform its work in accordance with the National Electric Contractors Association (NECA)/Building Industry Consulting Service International (BICSI) 568 standard which defines minimum requirements and procedures for installing telecommunications cable infrastructure, including balanced twisted-pair copper cabling and fiber optic cabling. This standard also describes professional workmanship.

The contractor shall:

a. Provide on-site coverage for all cabling maintained by the Cable Plant Technical Support Team.
b. Maintain cable infrastructure labeling standards IAW USCENTCOM developed policies, regulations, and procedures.
c. Maintain physical cable diagrams and database for HQ and CFH (Section F, Deliverable 2.21).
d. Develop and maintain inter and intra-facility/building layer-1 topology documentation. (Section F, Deliverable 2.22).

C.5.2.2 SUBTASK 2 – ENTERPRISE SERVICES SUPPORT (CCJ6-SE)

The contractor shall provide the following support for all of the tasks/subtasks in the Enterprise Network Services area:

a. Provide onsite support for systems/services operated and maintained by the Server Maintenance Team and the Global Command and Control System (GCCS) Technical Support Team.
b. Prepare, update, and maintain accreditation packages for new or existing systems and equipment.
c. Maintain and publish current network information to include trend analysis of common problems and system performance, average device and service uptime, service outage durations and frequencies, trouble ticket status updates, and other parameters identified by the PM.
d. Monitor servers, applications, and services to facilitate early detection of incidents, impending outages or degradations.
e. Determine COAs, develop drawings, provide cost and time estimates, generate assembled material lists, and create documentation in support of GCCS installations, End-User IT System installations, and Wireless Communications installations.
f. Develop and publish best practices, policies, and procedures on all aspects of the Defense Messaging System (DMS) Family of System (FoS) environment, the GCCS FoS environment related to this task.
g. Support all USCENTCOM Contingency Operations, to include initial installations at Component sites in support of these operations.

C.5.2.2.1 GLOBAL COMMAND AND CONTROL SYSTEM (GCCS) SUPPORT

The contractor shall be responsible for ensuring system availability and reliability of the Global Command and Control System - Joint (GCCS-J) and related GCCS Family of Systems (FoS) on U.S. and Coalition networks at HQ USCENTCOM and CFH. The contractor shall provide technical support to USCENTCOM and all USCENTCOM Joint Task Force (JTF) and service components in the AOR. The contractor shall plan, develop, and implement GCCS program requirements. The contractor shall be responsible for maintenance, troubleshooting, installation, configuration, and the implementation of existing and future versions of the GCCS FoS.

The contractor shall provide system administration support, technical support, and subject matter expertise for GCCS FoS including, but not limited to:

a. Common Operational Picture (COP)
b. Integrated Imagery and Intelligence (I3)
c. NEWSGROUP Servers for Joint Operation Planning and Execution System (JOPES)
d. IA and Client/Server installation
e. Theater Ballistic Missile Defense (TBMD) and various GCCS-J subsystems

The contractor shall:

a. Provide management, system administration, planning, and operational support for all Command and Control servers and client assets, including UNIX systems, within the scope of this task.
b. Provide a Weekly Activity Report (WAR) on GCCS-related activities (Section F, Deliverable 2.23).
c. Provide a quarterly report on the status of GCCS COOP capabilities (Section F, Deliverable 2.24).
d. Directly administer GCCS FoS assets employed at HQ USCENTCOM and provide technical support to deployed units in USCENTCOM's AOR.
e. Perform Configuration Management and Project Management and ensure IA compliance for all USCENTCOM GCCS FoS assets.
f. Conduct GCCS acquisition planning activities to include upgrades, enhancements, and replacements of software and hardware.
g. Perform any necessary actions required to respond to GCCS FoS problem reports.
h. Perform system, security, and operational testing/evaluation events in coordination with Joint Staff (JS) J3 and GCCS-J PMO to determine suitability to field for future releases.
i. Ensure USCENTCOM personnel and contractors are trained on the GCCS FoS server-based systems and maintain a recurring training program.
j. Manage and administer the Radiant Mercury Cross Domain Solution (CDS) or other designated CDS in support of the USCENTCOM GCCS mission.

C.5.2.2.2 SERVER MAINTENANCE SUPPORT

The Server Maintenance program ensures that key and supporting services are reliable and available to end users when needed. The contractor shall establish and operate a Server Maintenance program that provides systems administration, maintenance, computer security

compliance, and support for servers on all USCENTCOM networks, as well as those at SCO locations throughout the USCENTCOM AOR and those on Allied and Coalition networks. The contractor shall also operate and maintain items such as servers (physical and virtual), firmware, operating systems, software, and Storage Area Networks (SANs). The Server Maintenance Program supports HQ USCENTCOM, multiple locations on MacDill AFB, sites within the Tampa Bay metropolitan area, other CONUS locations, CFH, and locations within USCENTCOM's AOR.

The contractor shall:

a. Provide day-to-day operations by maintaining, managing, monitoring, and administering server systems on USCENTCOM, Allied/Coalition, and SCO-based networks.
b. Maintain and administer all hardware, software, firmware, and operating systems for all systems within the scope of this task.
c. Provide server support for DoD IT services at U.S. Embassies within the scope of this task.
d. Perform capacity planning and allocate disk space.
e. Provide server support for the USCENTCOM COOP. This support shall include participation in training activities, exercises and real world deployments. In the event of a real-world emergency, COOP support may be required for extended periods of time.
f. Advise USCENTCOM regarding any required modifications or upgrades to server equipment and software.
g. Monitor servers, applications, and services to facilitate the early detection of incidents, impending outages, or degradations.
h. Provide server IA (i.e., Information Assurance Vulnerability Alert (IAVA) assessment compliance) (Section F, Deliverable 2.25), health (e.g., disk and central processing unit (CPU) utilization) (Section F, Deliverable 2.26) and status reports to the PM (Section F, Deliverable 2.27).
i. Ensure that the IT environment is accessible through the establishment and maintenance of user accounts, profiles, print and disk services, data file services, Domain Name services, and other means.
j. Provide aggressive computer security management to maximize server security posture. Monitor and review computer security scans, and implementation of security upgrades and applications.
k. Configure, manage, and maintain the USCENTCOM thin client architecture on all networks and systems within the scope of this task IAW USCENTCOM policies, regulations, and procedures.
l. Configure, manage, and maintain the USCENTCOM boundary security devices and architecture on all networks and systems within the scope of this task IAW USCENTCOM policies, regulations, and procedures.
m. Configure, manage, and maintain the USCENTCOM virtual computing infrastructure on all networks and systems within the scope of this task IAW USCENTCOM policies, regulations, and procedures.

n. Provide expertise and advice on server operations and maintenance to the USCENTCOM JCCC via a designated liaison.

C.5.2.3 SUBTASK 3 – CUSTOMER SUPPORT OPERATIONS (CSO) (CCJ6-SC)

C.5.2.3.1 INFORMATION TECHNOLOGY SERVICE DESK SUPPORT

The USCENTCOM Customer Support Operations (CSO) provides a centralized single point of contact for USCENTCOM end users to quickly and easily interface with IT customer service operations. The CSO performs troubleshooting of tickets in efforts to resolve issues quickly. The CSO also ensures accurate categorization, prioritization, routing, transfers, and data integrity of all applicable tickets. It ensures consistent incident, change, and problem life cycle processing. The CSO provides support to HQ CENTCOM, Washington Liaison Office (WLNO), CFH, and AOR customers.

The CSO interfaces with end-users via telephone calls, chat, remote desktop, automated requests, electronic mail, and other means. Additionally, the CSO provides walk-in support for customers at HQ USCENTCOM that have issues requiring face-to-face interaction, such as managing network accounts and resetting Common Access Card (CAC) Personal Identification Numbers (PINs), issuing and support of Secret Internet Protocol Router (SIPR) Token Cards. The CSO supports users on all applicable networks within the scope of this task. The CSO provides support to HQ USCENTCOM, WLNO, CFH, and AOR customers.

The contractor shall:

a. Maintain and enhance the CSO customer walk-in reception desk at HQ USCENTCOM that operates during normal duty days as defined by USCENTCOM.
b. Maintain and enhance the CSO CONOPS (Section F, Deliverable 2.28).
c. Provide Ticket Management support such as troubleshooting, recording, prioritizing, tracking, escalating, and contacting end users.
d. Identify, research, and resolve tickets within the scope of Tier 1 support capabilities. Tickets that require technical support or root cause determination that exceeds Tier 1 support capabilities shall be escalated to higher level support teams for expedient resolution.
e. Monitor and track the status of all submitted incidents, problems, and changes, including cases where they are escalated to higher levels of support (Section F, Deliverable 2.29).
f. Publish a weekly customer survey analysis report (Section F, Deliverable 2.30).
g. Recommend proposed fix actions to reverse negative trends. Perform follow-on trend analyses to assess the impact of any fix actions selected by USCENTCOM for implementation.
h. Review, edit, and maintain TTPs for CSO activities to execute and validate results of any tasks and processes within the scope of this task. These TTPs shall be published within 30 calendar days after TO award and updated as changes occur (Section F, Deliverables 2.10 and 2.12).
i. Identify trends in customer service and technical proficiency; take steps to improve service based on findings (Section F, Deliverable 2.31).

j. Update and maintain a knowledge base for investigating, diagnosing, and resolving Tier 1 incidents (Section F, Deliverable 2.32).

C.5.2.3.2 END-USER INFORMATION TECHNOLOLGY (IT) SYSTEM SUPPORT

The contractor shall provide O&M support for client computing devices to include personal computers, thin/zero clients, laptops, Portable Electronic Devices (PEDs), and peripherals. For all computer systems, peripherals, and other hardware devices within the scope of this task, the contractor shall establish a technical support program to install, maintain, upgrade, replace, and in the event of a failure or degradation in performance, analyze, troubleshoot, and restore systems/devices to operational status. The contractor shall coordinate and manage all equipment installations within the scope of this task.

The contractor shall:

a. Provide end-user IT system and software maintenance for the USCENTCOM COOP. This support shall include participation in training activities, exercises, and real world deployments. The deployable COOP communications capabilities to designated personnel in support to new missions and during emergency situations (e.g., hurricanes, fires, floods, cable cuts, power outages, equipment failures, etc.). In the event of a real-world emergency, COOP support could be required for extended periods of time.
b. Coordinate and manage Automated Data Processing Equipment (ADPE) accountability of new equipment, replacement equipment, and upgrades. The contractor shall also track the disposition of equipment throughout its life cycle (e.g., Computer Equipment Replacement Program (CERP) and Life Cycle Replacement (LCR)).
c. Process end of life, defective, and/or damaged equipment through the Defense Reutilization Management Office (DRMO).
d. Develop procedures to facilitate management and testing of desktop load set configurations to include tracking and compiling of user issues, software conflicts, devices conflicts, and other similar tasks.

C.5.2.3.3 WIRELESS COMMUNICATIONS

The contractor shall enhance and maintain a comprehensive Wireless Communications Program. Users on travel both CONUS and OCONUS shall be supported. The contractor shall provide all aspects of program maintenance, including the drafting of policies and procedures and the implementation and integration of new wireless services and technologies, as well as troubleshooting, repair, and logistical support for existing devices. The Wireless Communications team provides support to MacDill AFB, locations within the Tampa Bay metropolitan area, and other CONUS and OCONUS locations. Travel may be required to support service requests (CONUS and OCONUS) through TDY requests.

The contractor shall manage secure and non-secure wireless communications devices and associated auxiliary devices, wireless access points / controllers, and other user-operated wireless/auxiliary devices providing either network or cellular connectivity.

The contractor shall:

a. Provide on-site customer support for all systems/services operated and maintained by the Wireless Communications Technical Support Team.
b. Prepare, configure, test, troubleshoot, issue, and receive wireless communications devices and associated auxiliary devices.
c. Assist with managing all billing related to wireless communications devices, auxiliary devices, and services within the scope of this task.
d. Interface directly with customers to provide training and to resolve all issues related to services within the scope of this task.
e. Maintain utilization history to include review of device/service usage, audits, and reconciliation of utilization.
f. Maintain records on monthly billing and notices to Directorates/customers.
g. Provide USCENTCOM with monthly cell phone billing analysis that includes recommendations for reducing costs (Section F, Deliverable 2.33).
h. Interface directly with DISA for wireless service which includes management of USCENTCOM resources, providing training and resolving all issues related to services within the scope of this task.
i. Provide support for the USCENTCOM COOP. COOP support shall include participation in training activities, exercises and real-world deployments. The COOP provides deployable COOP communications capabilities to designated personnel in support of new missions and during emergency situations (e.g., hurricanes, fires, floods, cable cuts, power outages, equipment failures, etc.). In the event of a real-world emergency, COOP support could be required for extended periods of time.
j. Function as the Primary and alternate Personal Wireless Communications Manager.

C.5.2.3.4 VISUAL INFORMATION SERVICES (VIS)

The contractor shall provide and support Visual Information Services (VIS) which includes, but is not limited to, the setup, engineer, adjustment, and operation of video teleconferencing (VTC) devices, teleconferencing services, audio-visual (A/V) services, desktop collaboration services, public address (PA) systems, and multi-display clocks. The contractor shall provide robust VIS capabilities for HQ USCENTCOM and CFH meeting and conference facilities, as well as public events as required. The contractor shall support these services on Non-secure Internet Protocol Router Network (NIPRNet), SIPRNet, Coalition Partner Networks, and any Command-approved networks as requested by the Command.

The contractor shall:

a. Provide on-site end user support for mission-critical and mission-essential VIS systems/services operated and maintained by the VIS Technical Support Team. The contractor shall support all events outside of duty hours.
b. Integrate, test, maintain, and operate VTC and A/V suites and teleconferencing hardware and software.
c. Establish USCENTCOM VTC and A/V connectivity to other locations and equipment.
d. Schedule, coordinate, and administer multiple simultaneous VTC and A/V sessions.

e. Ensure that all PA systems and associated equipment are operational and capable of supporting events.
f. Support the distribution of digital signage and cable television within USCENTCOM facilities.
g. Maintain situational awareness of Joint Worldwide Intelligence Communications System (JWICS) VTC capability, report degradations and outages IAW USCENTCOM policy, and provide assistance to correct any problems or issues.
h. Provide support for the USCENTCOM COOP. COOP support shall include participation in training activities, exercises and real world deployments. The COOP provides deployable COOP communications capabilities to designated personnel in support of new missions and during emergency situations (e.g., hurricanes, fires, floods, cable cuts, power outages, equipment failures, etc.). In the event of a real-world emergency, COOP support could be required for extended periods of time.
i. Recommend upgrades to the VTC and AV systems at least annually and incorporate approved upgrades if/when acquired.
j. Monitor VIS services to facilitate the early detection of incidents, impending outages or degradations.
k. Schedule, configure, and connect USCENTCOM users to Global Video Services (GVS) conferences.
l. Provide Defense Collaboration Services (DCS) end-user support to new account holders and assist users in the use of the application.
m. Train both USCENTCOM and contractor personnel on the operation of A/V and VTC equipment.
n. Maintain a COMSEC account for key material necessary to run secure VTCs.
o. Provide customer support for cable and satellite television service requests.
p. Assist in the validation of cable and satellite television billing.
q. Install, configure, and maintain hardware and software on Command-approved networks as requested by the Command.
r. Provide engineering support and technical expertise on all audio visual products in HQ, design and maintain standards for the Tier 1; interfacing with DISA to coordinate engineering of Tier 1 to Tier 0 interface connections; addressing interoperability issues and requirements; planning, coordinating, and managing, Collation VTCs, Video Teleconferencing Over Internet Protocol (VTCoIP), SVTCoIP routing to the Department of Defense Information Network (DoDIN); and addressing routing issues.
s. Provide all programming for all new installs of VTC suites and any adjustment of current systems that are required by the Government within the scope of this task.
t. Provide normal and after hour Tier III engineering assistance for Audio Visual to include integration, programming, and testing of the solutions architecture.
u. Analyze and provide recommendations for the tailoring and use of operational process models based on accepted industry standards such as IT Infrastructure Library (ITIL)

v. Follow up with the customer to ensure that requirements are being met and whether or not there are additional systems that may need to be located and/or sourced.

C.5.2.3.5 TRAINING ACADEMY

USCENTCOM Training Academy offers certification-based training, end-user training, and proctors certification examinations. Certification-based training has the objective of preparing trainees to take the certification examination. End-user training provides application and systems training to the users, which enables them to execute required tasks. The contractor shall manage this customer training program covering IT skills required for end-users at USCENTCOM to effectively perform their duties. The contractor shall also manage a training program covering skills required for technical support teams to effectively perform their duties. Training shall be provided only to Government and Military personnel unless an exception is granted by USCENTCOM and GSA.

The contractor shall:

a. Provide on-site training based on USCENTCOM training requirements at locations designated by USCENTCOM. In certain cases, training may be conducted outside of scheduled duty hours (e.g., evenings or weekends). In addition, the training location may require the instructor to travel and deliver training to USCENTCOM users or technicians outside the installation.
b. Develop new training courses and materials and update existing materials that cover topics related to Information Systems (IS), IT, software applications, and other emerging technologies adopted by USCENTCOM.
c. Conduct periodic surveys to assess the training requirements of customers and provide a recommended curriculum for each quarter.
d. Based on the curriculum selected by USCENTCOM, update the training program on a quarterly basis to keep pace with changes in requirements (Section F, Deliverable 2.34). The training curriculum shall be implemented within five duty days after the start of each quarter.
e. Train USCENTCOM personnel on Command standard software applications, designated IS, and other subject areas and recommend if students require follow-on training in order to execute required tasks.
f. Support Division training meetings in order to obtain training requirements and identify training gaps that prevent technicians or end users from performing their duties.
g. Conduct courses utilizing new or revised material for trial group(s) of USCENTCOM personnel.
h. Develop training schedules (Section F, Deliverable 2.35).
i. Schedule students for classes and keep attendance records for all classes taught by the contractor.
j. Track and provide budgeting, forecasting, and consumption rate information in order to best utilize and manage training materials.
k. Develop, collect, and archive Course Customer Satisfaction Surveys to measure and perform trend analyses of the effectiveness of courses and instructors.

C.5.2.4 SUBTASK 4 – EXECUTIVE COMMUNICATIONS SUPPORT (CCJ6-SX)

The contractor shall provide O&M, network engineering, and customer support for mobile communications equipment, IS, and networks that support the Commander, Deputy Commander, USCENTCOM Very Important Persons (VIPs), and their staff members. The contractor shall also provide O&M and installation support for computer systems, communications, and any other supporting equipment located at the residences of the Commander, Deputy Commander, USCENTCOM VIPs and their staff members. The contractor shall provide specific detailed information needed to support the selection of hardware and software and the identification of implementation techniques/tools that provide efficient solutions for meeting current and future business needs. The contractor shall install, operate, maintain, and in the event of system/network outages, analyze, troubleshoot, and repair communications systems, IS, and network equipment to restore them to operational status. Communications/IS and networks that shall be supported include, but are not limited to, remote communications equipment, mobile and deployable network communication systems, strategic and tactical multi-channel satellite communication systems (including KU/GAN/BGAN/X band terminals), secure telephone equipment, video conferencing terminals, laptops, desktops, computer peripherals, and other equipment in support of executive communication capabilities. Travel to CONUS and OCONUS locations shall be required.

The contractor shall:

a. Provide on-call/on-site support for all systems/services/networks operated and maintained by the Executive Communications Technical Support Team which includes travel to CONUS and OCONUS and quarters. On-call support shall be provided during non-duty hours and holidays. The maximum time to respond to on-call support request is 20 minutes. The maximum time period for reporting to duty station after on-call support has determined that on-site support is required is one hour. A comprehensive on-call/alert roster shall be maintained and updated on a monthly basis.

b. Develop and publish best practices, policies, and procedures regarding methods and techniques for packing of equipment that minimize damage during transit as required (Section F, Deliverable 2.36).

c. Monitor mobile Executive Communications Team systems and network connectivity to facilitate early detection of incidents, impending outages, or degradations.

d. Maintain a minimum of 16 complete suites of deployable communications equipment for the Commander, Deputy Commander and USCENTCOM Executive Communications users. The equipment should be packed in the appropriate transit cases in accordance with work center instructions.

e. Periodically test all deployable communications suites at time intervals determined by the Performance Monitor to ensure all equipment is operational.

f. Load, unload, and install all communications equipment within the scope of this task on/off airborne assets and vehicles.

g. Provide and assist USCENTCOM with information on systems/equipment needed to support system life-cycle replacement planning and execution including procurement of

hardware, software, and necessary supplies for the sustainment of equipment and systems.

h. Support design and planning of mobile and deployable network communications systems.
i. Coordinate with the appropriate agencies to establish reach-back and long-haul circuit interconnections.
j. Provide support to the USCENTCOM COOP. This support shall include participation in training activities, exercises, and real world deployments. The COOP provides deployable communications capabilities to designated personnel in support to new missions and during emergency situations (e.g., hurricanes, fires, floods, cable cuts, power outages, equipment failures, etc.).
k. Install laptop load set configurations including unique user profiles on all relevant mobile kit components within the scope of this task and update and modify these configurations or profiles as needed.
l. Integrate all hardware and software within the scope of this task.
m. Maintain accurate inventory data of all equipment included in deployable communications suites and any spare equipment (Section F, Deliverable 2.37).
n. Coordinate and manage Automated Data Processing Equipment (ADPE) accountability of new equipment, replacement equipment, and upgrades. The contractor shall also track the disposition of equipment throughout its life cycle (e.g., CERP and LCR).
o. Process end-of-life, defective, and/or damaged equipment through the DRMO.
p. Deploy CONUS or OCONUS as needed in support of operations, conferences and COOP; support required for extended periods of time may be handled through surge (CLIN x001b).
q. Provide training to Executive Communication Team members on all communications equipment within the scope of this task.
r. Maintain graphical representation models of the Communications Networks, as required, to provide CENTCOM's Tier 2 monitoring tools suite a complete high-level overview of network performance and health reporting statistics of network infrastructure devices (Section F, Deliverable 2.16).
s. Maintain a COMSEC sub-account and accountability of key material necessary to operate secure networks and communications at all locations in accordance with Command COMSEC guidelines and all applicable directives. CRO will maintain folders and assist COMSEC users with proper documentation and accountability of all applicable COMSEC material.
t. Maintain cable infrastructure labeling standards in accordance with USCENTCOM-developed policies and procedures.

C.5.2.5 SUBTASK 5 – COALITION MISSION PARTNER SUPPORT (CCJ6-SP)

C.5.2.5.1 COALITION PARTNER NETWORK (CPN) SUPPORT

The contractor shall manage O&M for all bilateral CPN and USCENTCOM Combined Enterprise Regional Information Exchange System (CENTRIXS) South West Asia (CX-SWA).

The contractor shall manage O&M for all aspects of CPN and CX-SWA operation including, but not limited to, systems administration, maintenance, computer cyber security compliance, IT infrastructure support for all networks (Allied and Coalition) as well as those at SCO locations, voice, video-teleconference, and reporting key metrics on all Coalition Mission Partner networks operational and system activity. The scope of CPN systems and networks support HQ USCENTCOM, multiple locations on MacDill AFB, other CONUS locations, CFH, and locations within USCENTCOM's AOR.

The contractor shall:

a. Provide expertise and advice relating to CPNs, CPN-X, CX-SWA, and coalition networks, providing remote support as needed.
b. Monitor servers, applications, and services within the scope of this task to assess their network health and to facilitate early detection of incidents, impending outages, or degradations.
c. Coordinate between HQ USCENTCOM and USCENTCOM AOR sites pertaining to CPNs, CPN-X, and USCENTCOM CX-SWA issues.
d. Maintain and publish current CPN information to include trend analysis of common problems and system performance, average device and service uptime, service outage durations and frequencies, trouble ticket status updates, and other parameters identified by the PM (Section F, Deliverable 2.38).
e. Maintain graphical representation models of the logical CPNs, CPN-X, and USCENTCOM CX-SWA (Section F, Deliverable 2.16).
f. Troubleshoot issues with existing or developed systems and work with the appropriate resources to resolve them.
g. Coordinate with network system administrators to minimize network service disruption.
h. Provide support to the USCENTCOM COOP. This support shall include participation in training activities, exercises, and real world deployments. The COOP provides deployable communications capabilities to designated personnel in support to new missions and during emergency situations (e.g., hurricanes, fires, floods, cable cuts, power outages, equipment failures, etc.).
i. Develop, write, and edit material for reports, briefs, and related technical and administrative publications.
j. Oversee support as needed for all current and future CPN voice services and projects.
k. Provide end user training on CPN to USCENTCOM and Coalition Partners throughout the AOR. Language translation may be required for trainees.

C.5.2.5.2 SECURITY COOPERATION ORGANIZATION (SCO) SUPPORT

USCENTCOM is required to provide sustained C4 support for 17 SCO Offices located in U.S. Embassies throughout USCENTCOM AOR. The ultimate goal is to ensure data, voice, video, and communication requirements are correctly provisioned and operational to support assured communication between Commander USCENTCOM and Senior Leaders.

The contractor shall provide systems integration and installation support to 17 SCOs located in U.S. Embassies throughout USCENTCOM AOR. The contractor shall administer systems, perform

testing, perform training, and provide O&M support for computers, voice, video and communications at each SCO. The contractor shall utilize remote communications (e.g., electronic mail, telephone), as well as site visits to accomplish this task.

The contractor shall:

a. Provide remote support for all system/services operated and maintained within the scope of this task at SCO locations. On-call support shall be provided outside of these hours, with a maximum time for reporting to HQ duty station after on-call support is requested of one hour from time of notification. The contractor shall maintain a comprehensive on-call/alert roster and update this roster on a monthly basis.

b. Install, configure, and maintain SIPRNet and NIPRNet hardware and software (Note: NIPRNet instances service is required when the embassy does not have internal support).

c. Install, troubleshoot, repair, operate, and maintain computers, telecommunications, and network equipment to include workstations, servers, printers, scanners, cryptographic encryptors, telephones, and any other equipment within the scope of this task.

d. Provide life cycle management of SIPRNet and NIPRNet equipment IAW USCENTCOM Regulation 25-75, “Information Management Security Cooperation Organization (SCO) Information Systems Support.”

e. Perform site assistance visits of all embassies to perform preventative maintenance, training, and maintain 100 percent accountability of all assets within the scope of this task (Section F, Deliverable 2.3). Track and provide budgeting, forecasting, and consumption rate information in order to best utilize and manage spare equipment and ensure all necessary repair parts are available to quickly return assets to operational status . Visits shall be conducted at least once a year or as requirements emerge.

f. Provide the IS equipment inventory to USCENTCOM IAW Regulation 25-75.

g. Research and test new technology/systems to evaluate compatibility with current systems and make implementation recommendations. Assist SCOs in projecting future IS requirements as necessary.

h. Consolidate embassy communications test reports from other organizations into consolidated current status charts.

i. Monitor and test communication systems, networks, applications, and servers to facilitate early detection of incidents or impending outages or degradations IAW USCENTCOM Regulation 25-75. Coordinate as needed with USCENTCOM and external organizations to monitor and/or test communication capabilities.

j. Provide support for all embassy SCO equipment during site visits, to include: training, assistance, account management, software loads, hardware and software maintenance, cable runs, network administration, system administration, and COMSEC loads.

k. Maintain cable infrastructure labeling standards in accordance with USCENTCOM developed policies and procedures.

l. Provide reports, complete requests for new service, and recommend methodologies for installing new or upgraded communications circuits.

m. Perform system and data backups on SCO systems and servers IAW USCENTCOM back-up policies.

n. Update USCENTCOM SCO website to inform users in the AOR about events and important equipment-related information (Section F, Deliverable 2.40).
o. Assist USCENTCOM in capturing and preserving documents from the SCOs during annual records calls.
p. Provide updates to embassy phone lists (Section F, Deliverable 2.41).
q. Update instructions, network diagrams, inventories, regulations, guidelines, worksheets, spreadsheets, briefings, and checklists related to SCOs (Section F, Deliverable 2.42).
r. Conduct site visits to user locations at a minimum of once a year.
s. Maintain a COMSEC sub-account and accountability of key material necessary to operates secure networks and communications at all SCO locations in accordance with Command COMSEC guidelines and all applicable directives. SCO CRO will maintain folders and assist SCO COMSEC users with proper documentation and accountability of all applicable COMSEC material.

C.5.3 TASK AREA 3 – THEATER NETWORK OPERATIONS (NETOPS) SUPPORT

The contractor shall comply with the appropriate DoD-approved architectures, programs, standards, and guidelines, such as, the DODIN, Strategic Technical Guidance (STG), Defense Information Infrastructure (DII) Common Operating Environment (COE), Defense Information Systems Network (DISN), and Shared Data Environment (SHADE). Specific services addressed in this PWS are: Level 0 Fault Monitoring, Identification, Resolution, and Level 1 Current Operations Support.

C.5.3.1 SUBTASK 1 – LEVEL 1 CURRENT OPERATIONS FAULT MONITORING, IDENTIFICATION, AND RESOLUTION

The contractor shall support real-time operational configuration management and control of the USCENTCOM portion of the DODIN transmission; author, update, and disseminate Trouble Management Ticket reporting; coordinate, generate, direct, and staff ASIs to ensure state of health of DODIN networks; ensure timely and accurate status reporting for all DODIN links, trunks, circuits, and other systems to deliver the combatant component agencies across USCENTCOM AOR; reconcile outages/degradation/HAZCON reporting discrepancies between the various reporting agencies; and update and disseminate communications status reports.

The contractor shall provide current operations support and expertise for voice, data, transmission, and liaison between Combatant Commander, United States Cyber Command (USCYBERCOM), DISA (Global and Central), USCENTCOM Components, and JTFs, maintain situational awareness of USCENTCOM AOR network performance; and assist Components and JTFs with operational issues and NetOps reporting.

The contractor shall:

a. Detect current status and state change of select Tier 1 (Tier 0 to Tier 1 connectivity), and select Tier 2 network devices (current configuration and up/down).
b. Detect current status and state change of “Core” application services.
c. Correlate events of network devices and applications for system status.

d. Monitor logical network topology (connectivity and routing).
e. Evaluate and respond to event triggers.
f. Monitor network device and application performance.
g. Coordinate and prioritize changes for theater backbone (Tier 1, and select Tier 2 systems).
h. Execute approved changes, responses, corrective actions (where USCENTCOM has change authority) for Promina.
i. Coordinate approved changes where component has change authority.
j. Receive and assemble impact assessments regarding operations/intelligence/business missions by correlating operational events, and network status.
k. Generate reports using ticketing system (primary), email, phone, web portal posting, message traffic, and database entry (Section F, Deliverables 3.2, 3.3, 3.4).
l. Record and archive reports and store for trend analysis; generate rollup report (Section F, Deliverable 3.1).
m. Generate and disseminate situational awareness reports to higher, peer, and subordinate Network Operations (NetOps) Centers.
n. Perform trend analysis for network performance on Tier 1 devices and associated connectivity.
o. Validate configurations for Tier 1 and select Tier 2 devices and applications.
p. Escalate events/issues to appropriate Level 1 operators.
q. Maintain situational awareness of Tier 0, Tier 1, and select Tier 2 networks and perform proactive network analysis and health checks. Identify network problems; ensure strategic-to-tactical connectivity is functioning properly.
r. Advise the Chief Watch Officers and Operations Officer on the availability and performance of the theater architecture and recommend courses of action if required.
s. Assist components and JTFs with reporting and troubleshooting of issues.
t. Monitor and evaluate configurations and performance of the Tier 1 network.
u. Upon receipt of escalated network trouble conditions, recommend network recovery procedures to isolate specific trouble source.
v. Coordinate corrective actions to restore and repair network conditions to meet network availability goals and objectives.
w. Initiate, update, track, and close USCENTCOM-approved trouble tickets.
x. Document, track, and monitor incidents and problems to ensure timely resolution.
y. Process, validate, and determine impacts of Satellite Access Request (SAR)/Gateway Access Request (GAR) for connectivity.
z. Participate in engineering Defensive Cyberspace Operations (DCOs) and NetOps conferences (approximately on quarterly basis).
aa. Monitor logical network topology (connectivity and routing).
bb. Monitor network device and application performance.
cc. Support implementation of NetOps constructs and policies for USCENTCOM.

dd. Correlate events of network devices and applications for system status.

ee. Maintain situational awareness of changes for theater backbone (Tier 0, Tier 1, and select Tier 2 systems).

ff. Exercise COOP capability if required.

gg. Provide incident-related network optimization analysis (network improvement to optimize traffic and performance) and identify issues for detailed analysis by engineering cell.

hh. Maintain and update Functional SOPs (Section F, Deliverable 3.5).

ii. Audit tool configurations and network hardware/software inventories to validate comprehensive monitoring.

jj. Move/Add/Change (MAC) devices within monitoring toolset as they pertain to theater visibility. Configure monitoring and reporting tools (such as SOLARWINDS Network Configuration Manager), create custom scripts as necessary, and verify that Components have correct configurations to enable Tier 1 monitoring.

C.5.3.2 SUBTASK 2 – THEATER AUTHORIZED SERVICE INTERRUPTIONS

The contractor's duties and responsibilities include providing 24/7 management of all Inter and Intra Theater ASIs that affect the Tier 1 Theater Information Grid as well as authorized outages of Global Network Services that impact the CENTCOM AOR.

The contractor shall:

a. Provide tracking and coordination of intra/inter theater ASIs throughout the AOR.

b. Process component ASI requests and track all ASIs from initial requests to completion.

c. Provide ASI impact assessments of network systems, resolution to components with conflicting resources, and make recommendations to the Chief Watch Officer to assist in the approval process.

d. Verify ASIs for J6 Critical Information Requirements (CIR) status and reporting; complete ASI trouble tickets using USCENTCOM approved systems to provide reports for situational awareness and brief ASI status to JCCC Operations Chief.

e. Maintain and update SOPs (Section F, Deliverable 3.5).

C.5.4 TASK AREA 4 – ENGINEERING SUPPORT

C.5.4.1 SUBTASK 1 – PROGRAM PLANNING AND MULTI-NATIONAL MISSION PARTNER SUPPORT (MNMP)

C.5.4.1.1 PROGRAM PLANNING SUPPORT

The contractor shall provide support to J6 strategies in meeting the mission in providing net-centric solutions for the warfighter. This includes implementing a program to properly integrate new systems into USCENTCOM and aid in coordination of actions across the AOR. The contractor support shall increase visibility into life cycle management issues for maintaining existing systems and fielding new IT systems. The contractor shall coordinate, plan, and integrate IT systems in the procurement process, and shall focus on matching requirements

(capability) with resources (finances) for the short-term and creating a more cohesive long-term plan to serve both the Command and AOR elements.

The contractor shall:

a. Advise the CIO regarding a net-centric enterprise approach to IRM and IT application within the command.
b. Coordinate, develop, and evaluate governing policies needed to provide flexible and effective IT services and capabilities.
c. Support the Technology Innovation team to ensure the strategic plan is supported by the latest in proven advanced technology by monitoring, assessing, and evaluating emerging technological solutions.
d. Analyze integration effort to ensure compatibility and functional performance compliance to the requirements in consideration future projects or upgrades. Identify projected shortfalls and recommended corresponding solutions.
e. Develop comprehensive strategic engagement efforts to shape Service and DoD-level programs in support of USCENTCOM's mission requirements.
f. Support the CCJ6 DCIO to facilitate the development, submission, and synchronization of all Program Objective Memorandum (POM) data with the military services for all program area systems, applications, and IT capabilities within the USCENTCOM HQ and theater to ensure continuity of capability. Facilitate the development of initial Project Management Charters (PMC), kick-off briefings, and project scope statements.
g. Synchronize Joint/DoD, and Service-level technology insertions via a network of HQ, Service component, and Joint Task Force (JTF) project managers to achieve continuity of capability within the AOR.
h. Produce decision and information briefings/papers and status frameworks for all applicable programs, projects or processes (Section F, Deliverable 4.1).
i. Support the Engineering Branch to perform detailed systems analysis to support the development of operational/functional, systems, and technical architectures.
j. Coordinate and review detailed Certification and Accreditation (C&A) documentation in accordance with the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) or emerging DIACAP process (i.e., RMF).
k. Analyze risks and develop accompanying mitigation plans to support theater-wide technology insertions.
l. Coordinate and review Quality Assurance and Testing Plans to ensure interoperability with current USCENTCOM C4 baseline.
m. Coordinate and synchronize technology insertion efforts with the Joint Staff, DISA, Military Services (U.S. Army (USA), U.S. Air Force (USAF), U.S. Navy (USN), and U.S. Marine Corps (USMC)) and subordinate service components and JTFs in theater.
n. Develop, synchronize, and coordinate theater-wide implementation plans to ensure unity of effort within the entire theater.
o. Review and make recommendations on component and Combined Joint Task Force (CJTF) C4 network plans and network changes.

p. Provide support to the Project Team (C.5.4.2):
    1. Develop project plans in support of project managers (C.5.4.2) for technology insertion projects (Section F, Deliverable 4.1).
    2. Develop project-level resource and procurement strategies via a financial plan to execute technology insertion projects.
    3. Document CCJ6 C5 Program lessons learned (Section F, Deliverable 4.1) in accordance with CCJ6 policies and procedures.
    4. Transition technology insertion to full operational capability with defined change control processes properly articulated in applicable USCENTCOM regulations in coordination with Operations.
    5. Produce decision and information briefings/papers and status frameworks for all applicable projects or processes.
    6. Develop integrated program control processes for all technology insertions prior to transition to operations and maintenance activities.
    7. Develop management structures to ensure all manpower and support relationships are well-defined to support implementation and transition to operations and maintenance.

C.5.4.1.2 MULTI-NATIONAL MISSION PARTNER SUPPORT (MNMP)

The MNMP development effort supports the immediate Combatant Command Coalition Operations. Examples of Mission Networks in support of MNMP systems include, but are not limited to, CPN, CPN-X, and Combined Enterprise Regional Information Exchange System – Southwest Asia (CENTRIXS-SWA). These systems enhance the U.S. forces' defense posture and force protection and provide a significant resource for USCENTCOM to use in peace, crisis, war, and operations other than war by allowing collaboration through the sharing of information, e-mail, chat, and common operational picture.

The contractor shall:

a. Provide on-site program management and coordinate system engineering and technical support necessary to ensure full operational capability of the existing MNMP nodes at USCENTCOM and their associated forward sites.
b. Support operational expansion efforts within USCENTCOM AOR
c. Provide program management, reviews, development, integration, and coordination of installation necessary to support on-going development of the CENTRIXS Cross Enclave Requirement (CCER), and Mission Networks such as CPN and FMN, and applicable CDS that support MNMP.
d. Analyze the technical impacts of software/hardware maintenance enhancements and/or modifications to the system product baseline and provide technical reports.
e. Coordinate site survey, procurement, design, development, communications engineering, installation, implementation, and testing to establish MNMP capabilities within USCENTCOM's AOR.

f. Develop technical reports for each site surveyed with the definitive agreements, plans, and problem areas necessary to ensure a smooth installation into each location (Section F, Deliverable 4.13).
g. Ensure the configuration documentation is developed for each location.
h. Evaluate COTS/GOTS products, make recommendations, and support the implementation of new, improved system functionality and/or provide new functionalities in response to user-generated requirements.

C.5.4.2 SUBTASK 2 – PROJECT MANAGEMENT

The USCENTCOM J6 provides comprehensive management of IT, telecommunications, and other projects that align with the Command's strategy. The contractor shall provide assistance in the management of required projects that arise during the period of performance and within scope of the TO. Activities are required to follow the processes, phases, and standards in accordance with project management industry standards. These phases may include, but are not limited to, initiation, planning, execution, monitoring, closing and all applicable processes contained within each phase as they apply to each project. The contractor shall provide the project management deliverables specific to each phase of project management. The contractor shall track the acquisition and fielding of engineered solutions for HQ USCENTCOM, CFH, and the USCENTCOM AOR. The contractor shall liaison with USCENTCOM J6 Divisions to provide project coordination and support.

The contractor shall:

a. Provide project management using best industry practices in the Project Management Institute's (PMI) Project Management Body of Knowledge (PMBoK).
b. Facilitate the generation of project management deliverables within the Initiation Phase (Section F, Deliverable 4.1) (e.g., Charter, Information Paper, and Stakeholders documents).
c. Facilitate the generation of project management deliverables within the Planning Phase (Section F, Deliverable 4.1, 4.5, 4.7, 4.8, 4.9, 4.10, and 4.11) (e.g., Requirements document, Project Plan, Test Plan/Results, and Implementation Plan).
d. Facilitate the generation of project management deliverables within the Execution Phase (Section F, Deliverable 4.1, 4.7, 4.8, 4.9, 4.10, and 4.11) (e.g., Procurement Documents and Project Brief).
e. Facilitate the generation of project management deliverables within the Monitoring Phase (e.g., Scope/Pilot Results, Business Rules, and Operational Level Agreement/Memorandum of Agreement).
f. Facilitate the generation of project management deliverables within the Closing Phase (Section F, Deliverable 4.1, 4.8, 4.9, 4.10, 4.11) (e.g., Finalized Procurements, Final Project Acceptance, Project Closure Document, and Lessons Learned documentation).
g. Identify Key Stakeholders, risks, issues, update requirements document, and facilitate kick-off meeting with meeting minutes for projects within 10 workdays after project assignment.

h. Develop initial project schedule, determine milestone, and establish the timeline for project within 20 workdays of project kick-off (Section F, Deliverable 4.1).
i. Develop project review read-ahead at least 24 hours in advance of project status meetings.
j. Meeting minutes will be provided for all meetings within three working days after the meeting has been held. (Section F, Deliverable 4.12)
k. Coordinate with project stakeholders and comply with policy and with strategic objectives, policies, and portfolio plans for projects.
l. Coordinate with Division and Branch Chiefs on specific project requirements for clarity of scope of projects.
m. Perform Risk Management throughout the project life cycle for projects - identify/analyze/mitigate, accept, or ignore.
n. Create and maintain qualified project schedules, templates, and reports through the use and collaboration of Microsoft (MS) Project, MS Office Products, and MS SharePoint automated tools for all assigned projects.
o. Coordinate with Cyber Division for all IA accreditation requirements for all projects.
p. Coordinate with CCJ6 Office of the (CIO) for all portfolio management requirements.
q. Coordinate with Resources and Analysis Division to provide procurement documentation.
r. Coordinate with Change/Configuration management for technical assessment and configuration control.
s. Track the fielding/installation of procured hardware/software solutions.
t. Prepare and maintain Action Officer-level project status brief of all projects currently managing.
u. Attend Division-level meetings as scheduled by Division or Deputy Chief to provide project management input as required.
v. Develop kick-off briefings and project scope (requirements) documents.

C.5.4.3 SUBTASK 3 – ENGINEERING COMMUNICATIONS

The contractor shall provide Engineering Design and Architecture support and shall be responsible for providing enterprise engineering support and expertise for voice, data, and transmissions networks in the USCENTCOM AOR. The contractor shall develop engineering solutions and COAs to assist CENTCOM supported Commanders with the integration of new C4 technology to include HQ, theater, and all future CENTCOM sites. The contractor shall be responsible for Tier III troubleshooting of digital and analog voice, data, visual information services, and transmissions networks for HQ. The contractor shall be responsible for evaluating and reviewing the effect of architectural changes on the Technical Implementation Guide (TIG). The contractor shall perform support in accordance with industry best practices.

The contractor shall:

a. Provide planning and engineering guidance to component network planners at CENTCOM directed engineering conferences.

b. Conduct gap analysis and identification in policies and CONOPS on a bi-annual basis.
c. Perform C4 network planning for contingencies, exercises, and current operations.
d. Provide detailed planning of C4 network changes to support emerging theater C4 requirements.
e. Review, edit, publish, and maintain documentation (written and graphical) of all engineering and design activities (to include design and implementation plans) of the USCENTCOM networks (Section F, Deliverables 4.24 and 4.25).
f. Identify theater requirements for strategic assets (e.g., strategic satellite terminals, strategic voice switches, strategic multiplexers, and strategic data routers).
g. Identify re-utilization/re-allocation of strategic theater assets based on requirements.
h. Provide design/architectural recommendations (e.g. white papers) for long-term/chronic problem resolution (Section F, Deliverable 4.23).
i. Provide normal and after hour Tier III engineering assistance, to include data networks, audio visual, transmissions, and telephony to include integration, programming, and testing of the solutions architecture.
j. Support the planning, execution, and after-action phases of current operations, contingency operations, exercises, and joint network upgrades in the USCENTCOM AOR.
k. Evaluate and recommend updates to the circuit actions database.
l. Validate SATCOM requirements through Defense Information Technology Contracting Organization (DITCO), including military and commercial providers.
m. Manage all Satellite Access Requests (SAR), Gateway Access Requests (GAR) and Requests for Services (RFS), including direct coordination with Component and Joint Task Force Commanders and DISA organization to ensure smooth, seamless processing of all requirements
n. Maintain databases and web pages.
o. Provide planning and engineering for contingency operations for all communications networks.
p. Ensure engineering tasks and solutions comply with USCENTCOM accreditation, certification and connection standards for HQ's and theater's networks and systems, through working with the certification and accreditation branch.
q. Perform review, analysis, and documentation for the life cycle security requirements of applications, systems, and networks within the HQ USCENTCOM.
r. Review Security Test and Evaluation plans; modify or refine if necessary.
s. Advise the Theater Information Assurance Manager (IAM), Chief of C4 Plans and Operations, USCENTOM Certification Authority, and the Theater Designated Approval Authority (DAA) of network and system risks, risk mitigation, COAs, and operational recommendations.
t. Provide direct Tier III support and Tier IV liaison support (with manufactures) for digital and analog voice, data, visual information services, and transmissions network issues.

Track Tier IV escalations to completion. Document Tier III support issues via ticketing system.

u. Provide ticket accountability reports, as required.

v. Follow up with the customer to ensure that requirements are being met and whether or not there are additional systems that may need to be located and/or sourced.

w. Analyze and provide recommendations for the tailoring and use of operational process models based on accepted industry standards such as ITIL.

x. Maintain networking lab environment to best practice and USCENTCOM standards

y. Coordinate with USCENTCOM engineering for theater requirements strategic assets (e.g., strategic satellite terminals, strategic voice switches, strategic multiplexers, and strategic data routers).

z. Staff all service requests through USCENTCOM engineering and assign USCENTCOM validation prior to submitting through DISA Direct Order Entry (DDOE).

aa. Process tactical requests for service, generating a Tactical Telecommunications Service order (Tactical TSO), process DISA Direct Order Entry requests, generating a telecommunication service order (Strategic TSO).

bb. Maintain Command Communication Service Designator (CCSD) portal to include: all changes associated with reports In Effect Reports (IER), Delayed Service Report (DSR), etc.), strategic and tactical TSO's, Telecommunications Service Requests (TSRs)

cc. Perform validation for all telecommunication requirements within South West Asia (SWA).

dd. Conduct gap analysis and identification on Annex K and 5 OPLANS on a bi-annual basis.

C.5.4.3.1 DATA NETWORK ENGINEERING

The contractor shall be responsible for providing engineering support and technical expertise on all data network issues in theater; design and maintain standards for the Tier 1 data network in theater; interfacing with DISA to coordinate engineering of Tier 1 to Tier 0 interface connections; addressing interoperability issues and requirements; planning, coordinating and managing IP routing to the DISN backbone; and addressing network routing issues. The contractor shall provide network engineers to support the appropriate data communications components and configure them to meet user and USCENTCOM needs. The contractor shall support the construction of a reliable and high-performing network integrating Local Area Network (LAN), WAN, Internet, and intranet components entails network modeling and analysis.

C.5.4.3.2 TRANSMISSIONS ENGINEERING

The contractor shall be responsible for providing engineering and technical expertise on all transmissions network issues in theater; engineering and maintain administration of the transmissions network in theater (including military and commercial Radio Frequency (RF), SATCOM, and multiplexing systems). The contractor shall also interface and coordinate with commercial satellite vendors to obtain transmission plans. The contractor shall maintain

situational awareness of capacity availability over the AOR. The contractor shall validate telecommunication theater requirements in accordance with applicable directives.

C.5.4.3.3 CYBER SECURITY ENGINEERING

The contractor shall provide cyber security engineering in support of the CCJ6-C Cyber Support Task Area IA defense in-depth program for USCENTCOM enterprise networks. The contractor shall engineer the appropriate levels of security to ensure confidentiality, integrity, availability, and accountability have been established based on national and DoD security regulations and directives. The contractor shall provide security and information engineering support to HQ USCENTCOM, Theater Components, CFH, and JTFs. The contractor shall provide support to information technology security, focusing on protecting computers, networks and data from unintended or unauthorized access, change, or destruction.

C.5.4.3.4 TELEPHONY AND AUDIO VISUAL ENGINEERING

The contractor shall be responsible for providing engineering support and technical expertise on all telephony and audio visual products in theater and HQs; design and maintain standards for the Tier 1; interfacing with DISA to coordinate engineering of Tier 1 to Tier 0 interface connections; addressing interoperability issues and requirements; planning, coordinating and managing VoIP, SVoIP, VTCoIP, SVTCoIP routing to the DoDIN; and addressing routing issues.

C.5.4.4 SUBTASK 4 – TEST, ANALYSIS, AND INTEGRATION LAB SUPPORT

The USCENTCOM Test, Analysis, and Integration Lab is responsible for testing, analyzing, and integrating into production the technical solutions that meet USCENTCOM strategies.

The contractor shall provide solutions to unique production network and mobile communication issues. USCENTCOM's lab supports all the Command's unclassified, secret, and coalition networks, as well as mobile products. USCENTCOM must develop and integrate systems to support day-to-day garrison operations, as well as develop and maintain robust and survivable C4 systems.

The contractor shall test all hardware, software, and system configuration upgrades, additions, or revisions in the laboratory for Government approval before implementation. This includes downward-directed systems underwritten by the JS or other Government agencies. The contractor shall also perform comparison testing and associated test reports (Decision, Analysis, and Resolution) of similar products in order to determine which solutions are best suited to fulfill USCENTCOM requirements.

The contractor shall:

a. Provide testing, analysis, and integration including comprehensive lab integration documentation for USCENTCOM C4 initiatives (Section F, Deliverable 4.26).
b. Apply expertise on multiple aspects of computer network architectures on complex, cross-connected systems. Network expertise includes operational processes, hardware, software, and security.

c. Perform in-depth analysis of complicated systems to determine which are capable of supporting functional requirements and should continue to be used, which should be enhanced, and which should be replaced by more advanced designs.
d. Perform architectural planning integration and compliance testing of all hardware and software proposed for deployment within the USCENTCOM enterprise.
e. Create standard baseline image load set for all thick clients, Virtual Desktop Infrastructure (VDI) clients, and servers (Section F, Deliverables 4.27, 4.28, and 4.29).
f. Perform information security and IA assessments and recommendations to include IAVA, IAVM, and STIG applicability assessments and integration testing by suspense as mandated.
g. Provide direct Tier III and Tier IV liaison support for server, workstation, application, issues. Track Tier IV escalations to completion.
h. Build and maintain a variety of test bed environments (e.g., NIPRNet, SIPRNet, CPN, and others that may be needed in order to perform testing as well as evaluation and demonstration of new and current technologies).
i. Evaluate and respond to Change Requests and Problem Tickets as required.
j. Research and propose solutions to enable the modernization of the USCENTCOM IT architecture and integrate new technologies. Monitor emerging technologies and industry best practices and provide recommendation for IT refresh opportunities.
k. Develop and implement prototypes, proof-of-concept demonstrations, and hands-on engineering of management solutions.
l. Provide ongoing development for network/application toolsets and integration with other C4 systems.
m. Integrate monitoring systems to meet information exchange requirements.
n. Design, construct, test, and integrate hardware and software solutions, distributed computing solutions, and physical/logical communications networks.
o. Plan, integrate, and support existing network management systems employed in USCENTCOM Enterprise.
p. Evaluate COTS/GOTS products that could improve system functionality and/or provide new functionalities in response to user-generated requirements.
q. Provide status updates related to ongoing work orders and tasks to Government leadership through the use of reports as requested by Government customer.
r. Provide TTPs for all lab tasks.
s. Provide cyber security system support to ensure compliance and cyber due diligence within engineering to include Host Based Security and other disciplines as required. The contractor shall provide security and information engineering support to HQ USCENTCOM, CFH, Components, and JTFs.

C.5.4.5 SUBTASK 5 – SOFTWARE ENGINEERING SUPPORT

USCENTCOM is required to develop/integrate network web and databases systems, which provide support of day-to-day garrison operations. USCENTCOM CCJ6 provides direct

technical support, testing, systems integration, and web application development\ operations and maintenance support of USCENTCOM C4 Systems and Intelligence initiatives. The USCENTCOM Software Engineering Support Branch program develops and integrates systems to support day-to-day Government garrison operations, as well as transitions quickly to reliable wartime support for the CFH. Web/portal pages, databases, applications, and interfaces reside on SIPRNet, NIPRNet, and Coalition networks. It is necessary to ensure that the Command Software Engineering Branch possess the technical expertise to maintain web/portal capabilities, applications, and develop and maintain databases. The current code used for development includes Classic Active Server Page (ASP)\ASP.Net with Visual Basic and C#, JAVA script, and Transact Structured Query Language (TSQL). The contractor shall adjust to subsequent languages. The contractor shall be responsible for SQL databases and web applications/pages assigned or designated to this Task Area.

The contractor shall:

a. Provide engineering support with both locally developed software and COTS software in the Command.
b. Provide systems integration, testing, maintenance, installation, configuration, and troubleshooting for all databases and web/portal applications.
c. Provide SharePoint services, including architecture, configuration, and best practices. Design, implement, and maintain automated records management integration for SharePoint portal records (Section F, Deliverable 4.17).
d. Serve as technical Subject Matter Expert (SME) on database systems for the Command's SQL databases and multiple SQL servers.
e. Assist with monitoring operation of databases/web servers and ensures software and hardware are functioning properly and operational standards are met.
f. Provide technical guidance on the implementation of new web and database software.
g. Implement security and access controls requested by content owners.
h. Provide system design documentation for all systems and applications (Section F, Deliverable 4.14).
i. Work with USCENTCOM SMEs to capture business processes through customer interviews and finalizing requirements gathering.
j. Ensure architecture data integrity and consistent integration and conformity of products to the DoD standards. Support gathering, documenting, testing, deploying, and marketing of web content to support business processes within USCENTCOM.
k. Support web/database development and administration on the SIPRNet, NIPRNet, and coalition/allied networks throughout the AOR.
l. Provide technical support based on web policies stated in Office of the Secretary of Defense (OSD) Web Site Administration, DoD Instruction 5230.29, and DoD Directives 5230.9 and 5200.40.
m. Convert, migrate, and develop SQL databases to support Command's requirements Section F, Deliverable 4.15).

n. Develop, test, and implement web parts for the portals assigned or designated to this Task Area.
o. Provide policy and procedures for training users on new web/database applications.
p. Troubleshoot issues with existing or developed systems and work with the appropriate resources to resolve them.
q. Develop web base reports using SQL Reporting Tool for both locally developed applications and purchased COTS applications (Section F, Deliverable 4.16).
r. Write Stored Procedures, Views, and Triggers supporting database development.
s. Enforce automated standardization of Directorate/Agency web/portal pages with Command-level pages.
t. Develop web interfaces to Command and Directorate/Agency databases and files. Identify, recommend, develop, and implement solutions to customer requirements for greater availability to data and services hosted on web.
u. Assist in operation, maintenance and administration of web and portal servers, hardware, and software.
v. Coordinate software changes, following change management process, to minimize enterprise service disruption.
w. Develop and document management of web sites and provide input to web policy guidance for the Command.
x. Provide ongoing support, resolution of problems, and recovery of operational malfunctions involving hardware/software failure on web and database systems.
y. Coordinate with enterprise operations and ensure latest IAVA patches are loaded within the designated timeframe.
z. Identify and assign permissions and roles to databases and applications.
aa. Analyze database design and structure and recommend changes to improve performance.
bb. Provide training to application functional administrators.
cc. Document all upgrades to hardware and software within three workdays of upgrades.
dd. Keep database\web server documentation current to facilitate operational troubleshooting of systems.
ee. Meet with users and assist them create developing requirements packages for new applications. Consult with and advise managers and functional users in an effort to assist them define unique requirements necessary to meet their IT demands (Section F, Deliverable 4.18).
ff. Assist in completing a comprehensive, multi-disciplinary cyber security assessment addressing both content and technical issues at least annually on all web and database servers.
gg. Update incidents, work orders, and change requests at a minimum of every five workdays.
hh. Respond to customers within ten workdays after receiving a request for new software.

ii. Update information in the portal and develop a project plan and briefing if customer requests need major development not later than five workdays after first customer meeting.

jj. Ensure all new applications are developed mobile friendly to support future operations.

kk. Design, develop, maintain, and enhance applications software for the Combatant Command Joint Operations Center (JOC), responsible for maintaining situational awareness and joint operations across the AOR (Section F, Deliverable 4.21).

ll. Perform in-depth analysis of complicated systems to determine which are capable of supporting functional requirements and should continue to be used, which should be enhanced, and which should be replaced by more advanced designs.

mm. Maintain development standalone network where all software is designed, tested, and code is stored in a repository (Section F, Deliverable 4.19).

nn. Maintain offsite disaster recovery\COOP of development source code repository (Section F, Deliverable 4.20).

oo. Design, implement, and maintain automated records management integration for SharePoint portal records.

C.5.4.6 SUBTASK 6 – ENGINEERING AND NEW TECHNOLOGY SUPPORT

The role of the CCJ6 Engineering Division (J6-E) is that of the primary interpreter of operational technologies, issues, and decisions. The J6-E office is responsible for monitoring, assessing, and evaluating technology, and recommending appropriate technology solutions to support the policies and directives issued by the OCIO and in support of USCENTCOM J6 strategic plans and initiatives. USCENTCOM specifically requires systems engineering and technical integration support for technology insertions in support of the USCENTCOM mission. The contractor shall plan, coordinate, and integrate IT systems into the into the USCENTCOM HQs infrastructure with primary focus on Life Cycle Management and the procurement process: The contractor shall focus on matching requirements (capabilities) with resources (finances), generating and managing a technology innovation plan for the HQ's Command and its component Commands.

The contractor shall:

a. Provide guidance as SMEs, shaping the USCENTCOM C4 technical posture.

b. Provide technical integration tasks to include testing and evaluating system architectures/engineering design.

c. Recommend technical solutions to system shortfalls, emerging technologies, or proposed projects.

d. Provide technical guidance for the development of Information Resource Management (IRM) strategy and policies.

e. Evaluate new technologies in accordance with the USSCENTCOM Regulation (CCR) 25-200 process.

f. Research and propose solutions to enable the modernization of the USCENTCOM IT architecture and integrate new technologies. Monitor emerging technologies and industry best practices and provide recommendations for IT refresh opportunities.

g. Research, review, analyze, and recommend technology solutions to ensure the security and protection of USCENTCOM's information resources.
h. Identify and recommend business process improvements through the application of technology.
i. Plan, coordinate and establish near-term and long-range goals and objectives that provide the foundation for C4 technical products, services, and methodologies and ensure these are written into appropriate contracts, Service Level Agreements (SLAs), etc.
j. Gather technology requirements from J6 Directorate for evaluation.
k. Support the Information Technology Configuration Advisory Control Board (ITCAB).
l. Coordinate, review, analyze, and draft responses to DoD, OSD, JS, USCENTCOM, and Directorate tasks IAW USCENTCOM staffing procedures and guidance.
m. Assist in the planning process to integrate new systems in the theater architecture.
n. Maintain the Technology Roadmap for the J6 Commander to include documenting enterprise hardware/software currently in the system, when decisions need to be made, and when to review new technologies (Section F, Deliverable 4.30).
o. Research new and emerging technologies that could replace end-of-life/end-of-service technologies before they expire or renew.
p. Consolidate requirements to minimize redundant technologies and ensure that they are technically relevant to the mission of the Commander.
q. Represent the USCENTCOM at DoD and Industry events to include conferences, summits, and symposiums (approximately 12 – 15 events per year).
r. Provide System maps that connect the different technologies to enterprise services; eliminating the undesirable effects of changing technologies that impact other systems (Section F, Deliverable 4.31).
s. Performs initial assessments on new technologies before bringing them to the attention of leadership; eliminating the overwhelming amount of technology available to the customer.
t. Coordinate with the Acquisition and Resource Division to provide procurement documentation, Bill of Material (BOM), Statement of Work (SOW), vendor quotes, brand name justification, and sole source justification.
u. Prepares reports and recommendations of advanced technologies applicable to CENTCOM's mission by addressing gaps, reducing costs, and increasing security; conduct in-depth analysis and reports on data center storage technology and virtual server infrastructure.
v. Provide technical support for the J8 Science and Technology Branch for emerging and innovative technologies.

C.5.5 TASK AREA 5 – CYBERSECURITY

The contractor shall provide DCO Internal Defensive Measures (IDM) for HQ and theater operations, and HQ Cybersecurity Policy, Programs and Compliance support. In support of the tasks/subtasks, the contractor shall perform the following management and operations functions:

a. As required, prepare and provide cybersecurity risk and/or threat briefs to USCENTCOM leadership.
b. Implement a multi-tiered cybersecurity risk management program to protect USCENTCOM (to include CENTCOM Forward locations) interests, operational capabilities, and organizations information systems assets IAW National and DoD Cybersecurity regulations and standards.
c. Conduct trend analysis and publish summary reports on a monthly basis on DCO operations and Tasking Orders (TASKORD) analysis (Section F, Deliverable 5.1).
d. Develop and maintain a continuity of operations (Continuity Folder) to include checklists, standard operating procedures, and documentation pertaining to all systems and technologies relevant to this task area to facilitate training (Section F, Deliverable 5.2).
e. Provide subject matter expertise required to respond to Taskers.
f. Develop and publish best practices, policies, and procedures within the scope of each specified task (Section F, Deliverable 5.3).
g. Provide WAR and Weekly Status Reports (WSR) (Section F, Deliverable 5.4).
h. Perform organizational Records Management requirements and mandates.
i. Participate and attend mission-related conferences, events, and exercises as required.
j. Support Building Partner Capacity efforts and events.
k. Develop and maintain an information management mechanism for operations (currently via SharePoint).
l. Support Command Mission Assurance initiative and guidance.
m. Develop, track, and maintain the TASKORD and Communications Tasking Orders (CTO), tracking tool.
n. Track status and compliance with any actions associated with DoD-directed Force or Cyber Protection Condition levels.
o. Participate in working groups to include National and DoD-level Operational Planning Teams (OPT).
p. Respond to Requests for Information (RFIs).
q. Develop and maintain Command Defense-In-Depth Measures CONOPS and Architecture.

C.5.5.1 SUBTASK 1 – HQ DEFENSIVE CYBER OPERATIONS

The contractor shall provide 24/7 passive and active DCO IDM to protect, detect, analyze, and mitigate threats, to include insider threats, and respond to unauthorized activity within the accreditation authority of the USCENTCOM Authorizing Authority information systems, infrastructure, and networks. DCO-IDM protection activities shall be consistent with National, DoD, and Command cybersecurity principals, policies, and directives, and includes deliberate actions taken to modify an assurance configuration or condition in response to computer network defense alert or threat information.

Additionally, the contractor shall participate in DoD and Command-level Cyber security current operations including, but not limited to, working groups, use cases, tiger teams, email, chat, ticketing, and collaboration session communications. The contractor shall assist with collaborative theater cyber security planning and operations.

Within the enterprise, the contractor develops and maintains an effective and relevant enterprise cybersecurity training and awareness program that follows Federal, DoD, and USCENTCOM policies, regulations, and standards.

All personnel performing functions related to this task shall be certified in accordance with DoD 8570 (and all superseding policies and regulations). Tier 2 personnel will provide On-the-Job (OJT) training to Tier 1, and Tier 3 will provide OJT to Tier 2 and Tier 1 personnel to ensure continued improvement on all Tiers.

C.5.5.1.1 HQ DCO-IDM INCIDENT RESPONSE TIER 1 AND 2

The contractor shall support the employment of 24/7 Security Operations Center (analyst support) Tier 1 and 2. The primary functions provided by the team members shall be focused on DCO-IDM activities for preventing, detecting, analyzing, and responding to cyber security threats, events, remotely exploitable vulnerabilities, incidents or data breaches, the response to these events or incidents (after the necessary triage phase) and, at last, the remediation of the consequences of every detected event or incident. All of the actions must be coordinated through the USCENTCOM C4 Systems Directorate (CCJ6) Joint Cyberspace Communications Center.

The contractor shall:

a. Provide 24/7 onsite coverage of all network locations owned by the Authorizing Official for basic network and host event and log analysis (Tier 1) and incident handling and response (Tier 2).
b. Provide proactive measures for the prevention of cybersecurity incidents, including but not limited to: monitor, track, mitigate, and report computer network events or hostile indicators reported (CATs 1-8); continuous threat analysis; network and host scanning for vulnerabilities; countermeasure deployment coordination; and security policy and architecture consulting.
c. Fuse operational and intelligence-based cyber threat information and other information sources to provide predictive warning, threat analysis, and course of action recommendations to support current and long-term network defense mitigation strategies, as well as collaboration with the information operations community of interest for HQs.
d. Develop, maintain, and execute incident handling and response actions in accordance with DoD instruction, best security practices, and USCENTCOM policies.
e. Respond to confirmed incidents, by coordinating resources and directing use of timely and appropriate countermeasures.
f. Maintain internal incident tracking database.
g. Report Commander’s Critical Information Requirement (CCIRs), Priority Intelligence Requirements (PIRs), and other information requirements IAW USCYBERCOM, USCENTCOM, CCJ6, and Information Systems Security Management (ISSM) requirements and IAW SOP/TTPs. Perform trend analysis of security logs and events.

Based on the analysis, identify areas that need improvement, recommend security controls and best practices that should be implemented to mitigate any security problems and vulnerabilities detected.

h. Assist with the collection of cyberspace threat information originating from various sources such as law enforcement community products, databases, websites, and tools; commercial/open source products, databases, websites, and tools; locally generated databases, websites, and tools; and National and DoD sources of information.
i. Provide situational awareness and reporting on cybersecurity status, incidents, and trends in adversary behavior to appropriate organizations. Other relevant sources of information.
j. Disseminate cyberspace information to decision makers, as well as the cyber security, NetOps, and information operations communities to support planning, operations, and other related activities.
k. Create and deliver the daily DCO-IDM Briefs for the J6 and Operations staff (Section F, Deliverable 5.5).
l. Maintain and update DCO-IDM TTPs/SOPs (Section F, Deliverable 5.6).
m. Recommend changes to policy, procedure, or technology relevant to improvement of theater cyber security posture and capabilities.
n. Provide SME support to Operational Planning Teams and planning tasks assigned to the Cybersecurity Branch; support JS and USCENTCOM taskers and RFIs (with Government approval).
o. Perform information gathering and real-time analysis of theater Cybersecurity data from appropriate situational awareness and management tools.
p. Maintain Cybersecurity sensor grid situational awareness from Tier 0 to Tier 1 & 2; report sensor grid outages and/or anomalies.

C.5.5.1.2 BOUNDARY PROTECTION CELL

The contractor shall:

a. Monitor, detect, and analyze potential intrusions in real time and through historical trending on security-relevant data sources.
b. Analyze logs reported by network infrastructure devices, boundary and internal cyber defense sensors, host devices, correlated Security Information Event Management (SIEM) (e.g., ArcSight) events, syslog, and analytic tools within the scope of this task. Publish a report summarizing all findings on a weekly basis, or as required.
c. Receive, approve, and track all network and system security sensors (e.g., Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)/Firewall (FW)) requests.
d. Provide on-site support for operation, maintenance, and auditing on all FW and web proxies for all network locations owned by the Authorizing Authority.
e. Ensure FW Policies are configured IAW Ports, Protocols, and Services Management (PPSM) guidance.

f. Provide on-site support for operation, maintenance, and auditing on all host-based security suites, application whitelisting, and host-based logging on all network locations owned by the Authorizing Authority.

g. Develop, maintain, coordinate, and process Firewall Exception Rules (FERs) with AFCENT as appropriate.

C.5.5.1.3 ADVANCED CYBER DEFENSE AND INSIDER THREAT CELL

The contractor shall support the employment of the Advance Cyber Defense Cell and Inside Threat Cell. This support includes conducting incident analysis, process improvement, and advanced threat detection/ response.

Currently, the Advanced Cyber Defense capabilities team is considered the Tier 3 analyst component for incident response. The Tier 3 team is primarily composed of staff resources (Tier 1 and 2) that demonstrate initiative and have met all prescribed OJT requirements and skills to perform Tier 3 functions.

C.5.5.1.3.1 ADVANCED CYBER DEFENSE CELL

The contractor shall:

a. Provide advanced active cyber defense (Tier 3) hunt response operations by leveraging SIEM, host, network, dynamic data acquisition, and intelligence in order to identify, characterize, and counter adversarial cyber threats.

b. Identify, respond, and report security intrusions, security incidents/compromises, insider threats, and malware for all servers, clients, and other infrastructure within the scope of this task.

c. Review current intelligence for relevant threats and recommend appropriate actions/response.

d. Develop, maintain, and execute system policies, signatures, and correlated events to detect, mitigate, prevent, and report insider threats and/or cyber intrusions.

e. Perform network and system security audits IAW DoD instruction, best security practices, USCENTCOM policies, and regulations, to detect insider threats, malware and unauthorized access to USCENTCOM networks.

f. Develop, maintain, and execute a database of other-than-commercial malicious signatures to enable the detection of malicious activity during normal network operations, system and network scans, and hunt operations (Section F, Deliverable 5.7).

g. Perform advanced forensics collection and analysis on all networks and devices including system image analysis, system and network timeline analysis, and reverse engineering malware analysis within the scope of this task.

h. Utilize knowledge of packet analysis and network trending to establish a baseline of network traffic and determine if there are any internal/external cyber threats within the traffic.

i. Collect, process, and/or fuse information from all authorized cyber threat intelligence reports and outside agencies in support of indications and warning development to identify and attribute anomalous/malicious network activities.

j. Perform analysis of findings developed by External Adversary Hunt Cells during active cyber defense operations (Discovery Operations and Clearing Operations), develop metrics and trends to identify external cyber threat actors attempting to compromise IS at all network locations owned by the Authorizing Authority.
k. Document and forecast initiatives for External Adversary Hunt Operations (Section F, Deliverable 5.8).
l. Develop TTPs based on proven advanced hunt operations for 24/7 monitoring by the Tier 1 analysts (Section F, Deliverable 5.9).
m. Provide escalation support to component Cybersecurity Current Operations Watch Officers, and Cybersecurity staff members.
n. Recommend changes to USCENTCOM network surveillance resources based on cyberspace indications and warnings.
o. Conduct network, system, and web site vulnerability scans in support of current operations and continuous monitoring guidance.
p. Coordinate DCO and remediation actions with Command-assigned Cyber Protection Teams as required.

C.5.5.1.3.2 INSIDER THREAT CELL

The contractor shall:

a. Conduct Insider Threat Operations by leveraging host, network, dynamic data acquisition, and intelligence in order to identify, characterize, and counter Insider Threats.
b. Provide on-site support and on call response to operate, maintain, and audit User Activity Monitoring (UAM) tool for all for all network locations owned by the Authorizing Authority.
c. Perform analysis of findings developed by Insider Threat Cell during insider threat operations, develop metrics and trends to identify internal cyber threat actors attempting to commit espionage or attempting to compromise IS located at all network locations owned by the Authorizing Authority.
d. Document and forecast initiatives for Insider Threat Operations (Section F, Deliverable 5.10).
e. Conduct audit and data collection in support of Insider Threat cases.
f. Provide relevant data and briefing support to Command Insider Threat Program Office.

C.5.5.2 SUBTASK 2 – THEATER DEFENSIVE CYBER OPERATIONS

The contractor shall provide security management support for Cybersecurity and Strategic Enterprise Computer Network Initiatives. The objective of these tasks is to support USCENTCOM's efforts to direct and synchronize DCO that will proactively defend the USCENTCOM portion of the Global Information Grid (GIG), as well as to provide theater network security situational awareness to the USCENTCOM Commander.

The contractor shall fuse cyber threat information and other information sources to provide predictive warning, threat analysis, and course of action recommendations to support current and long-term network defense mitigation strategies, as well as collaboration with the information operations community of interest.

All personnel performing functions related to this task shall be certified in accordance with DoD 8570 (and all superseding policies and regulations). Tier 2 personnel will provide OJT training to Tier 1 and Tier 3 will provide OJT to Tier 2 and Tier 1 personnel to ensure continued improvement on all Tiers.

C.5.5.2.1 THEATER DCO-IDM INCIDENT RESPONSE TIER 1 & 2

The contractor shall:

a. Provide 24/7 on-site coverage for all systems/services operated and maintained by the Theater Cyber Initiatives Support Team.
b. Assess capabilities and gaps within theater network security posture; and document all recommended changes to sensors based on cyberspace indications and warnings.
c. Publish cyber security trend analyses of theater assessments, lessons learned, and recommended mitigation approaches within 30 calendar days of the completion of an assessment (Section F, Deliverable 5.11).
d. Provide 3 Tiered level analyst coverage for networks locations owned by the USCENTCOM Components operating within USCENTCOM AOR.
e. Provide proactive measures for the prevention of cybersecurity incidents, including but not limited to, monitor, track, mitigate, and report computer network events or hostile indicators reported (CATs 1-8); continuous threat analysis; network and host scanning for vulnerabilities; countermeasure deployment coordination; and security policy and architecture consulting.
f. Develop, maintain, and execute incident handling and response actions in accordance with DoD instruction, best security practices, and USCENTCOM policies.
g. Response to confirmed incidents by coordinating resources and directing use of timely and appropriate countermeasures.
h. Maintain internal incident tracking database and provide trend analysis of security logs and events (Section F, Deliverable 5.12).
i. Provide situational awareness and reporting on cybersecurity status, incidents, and trends in adversary behavior to appropriate organizations.
j. Report CCIRs, PIRs, other information requirements IAW USCYBERCOM, USCENTCOM, CCJ6 and ISSM requirements and IAW SOP/TTPs. Perform trend analysis of security logs and events. Based on the analysis, identify areas that need improvement, and recommend security controls and best practices that should be implemented to mitigate any security problems and vulnerabilities detected.
k. Assist with the collection of cyberspace threat information originating from various sources such as law enforcement community products, databases, websites, and tools; commercial/open source products, databases, websites, and tools; locally generated databases, websites, and tools; and National and DoD sources of information.

l. Disseminate cyberspace information to decision makers, as well as the cyber security, NetOps, and information operations communities to support planning, operations, and other related activities.
m. Create and deliver the daily DCO-IDM Briefs for the J6 and Operations staff.
n. Maintain and update DCO-IDM TTPs/SOPs.
o. Recommend changes to policy, procedure, or technology relevant to improvement of Theater Cybersecurity posture and capabilities.
p. Perform information gathering and real-time analysis of theater Cybersecurity data from appropriate situational awareness and management tools.
q. Maintain Cybersecurity sensor grid situational awareness from Tier 0 to Tier 1 report sensor grid outages and/or anomalies.

C.5.5.2.2 THEATER DEFENSIVE CYBER STRATEGY PROGRAMS

The contractor manages the production of cyberspace threat reports and products that support situational awareness, planning, operations, and response actions.

The contractor shall:

a. Contribute cyber-related tasks to all USCENTCOM operation orders, policy, and initiatives, to include a 48 to 72-hour quick response capabilities.
b. Provide subject matter expertise to assist with course of action development and implementation of an enduring DCO-IDM enterprise mitigation strategy.
c. Manage and respond to RFIs from USCENTCOM components, Information Assurance/Computer Network Defense (IA/CND) sections, and NetOps decision makers in order to support theater program initiatives.
d. Improve theater security posture by managing, tracking, and providing situational awareness for all USCENTCOM-directed strategic theater programs.
e. Provide DCO-IDM subject matter expertise to support planning, current operations, and security engineering activities.
f. Disseminate cyberspace information to decision makers, as well as the IA/CND, NetOps, and information operations communities to support planning, operations, and other related activities.
g. Assist with the collection of cyberspace threat information from the following sources:
    1. Law enforcement community products, databases, websites, and tools.
    2. Commercial/open source products, databases, websites, and tools.
    3. Locally generated databases, websites, and tools.
    4. Other relevant sources of information.

C.5.5.2.3 THEATER CYBER MISSION ASSURANCE

The contractor assists and supports the development and implementation procedures to identify critical assets and key terrain in cyberspace associated with the USCENTCOM Commander mission-critical functions. The contractor coordinates actions of cyber mission forces to identify

and mitigate vulnerabilities in key terrain. The contractor provides current cyberspace threat information through analysis and fusion of relevant operations and the Commander's priority.

The contractor shall:

a. Provide SME on mission assurance related policies and program to assist in the evaluation of risk to mission-based information systems.
b. Recommend technology upgrades and modifications based on evolving technologies, best practices, and strategic initiatives.
c. Recommend changes to USCENTCOM network surveillance resources based on cyberspace indications and warnings.
d. Produce and track the status of all Cyber Communication Task Orders (CTOs), fragmentary orders, Network Defense actions, and record messages.

C.5.5.2.4 THEATER CYBER PARTNER ENGAGEMENTS

The contractor shall develop, coordinate and champion activities that increase the defensive posture and knowledge of external entities. The contractor shall serve as a liaison officer between theater CND and assessment teams.

The contractor shall:

a. Coordinate the assessment of USCENTCOM Theater Component HQ and ensure their compliance with applicable DoD and USCENTCOM guidance. Publish an assessment schedule and create an executive summary of all findings and mitigation actions taken within 60 calendar days of the completion of each assessment (Section F, Deliverable 5.13).
b. Provide assessments brief to the USCENTCOM leadership personnel on the outcome of assessments conducted.
c. Create a repository of prior assessments conducted on components and all partners when applicable; to provide lessons learned and set conditions for future assessments.
d. Perform analyses of findings; develop metrics and trends to identify common theater security weaknesses.
e. Provide support to exercises and inject cyber related objectives when applicable to increase awareness and educate users.
f. Provide assistance to units prior to assessments to identify and when applicable mitigate any potential findings.

C.5.5.3 SUBTASK 3 – CYBERSECURITY POLICY, PROGRAMS, & COMPLIANCE

The contractor shall provide Cybersecurity policy and programs, vulnerability assessment and analysis, and network / system assessment and authorization (A&A) (IAW Risk Management Framework and/or current DoD standards) in support of the Cybersecurity defense in depth program for USCENTCOM enterprise networks. This shall include a complete and thorough risk assessment of all networks, information systems and applications to ensure these systems maintain the appropriate level of confidentiality, integrity, availability, and accountability based on national and DoD security regulations and directives.

The contractor shall:

a. Execute the Risk Management Framework program in accordance with DoD regulations and NIST guidance.
b. Develop, maintain, and execute a Continuous Monitoring Program IAW DoD requirements and National Institute of Standards and Technology (NIST) standards.
c. Perform risk/vulnerability assessments of systems, networks, and applications as required; advise leadership on network and system risks, risk mitigation, COAs, and operational recommendations as required.
d. Enforce, develop, and maintain authorization and assessment, and interconnection decision and standards for networks, systems, and applications.
e. Develop and maintain agreements, exceptions to policy, and waivers as required.
f. Perform network and system security audits IAW USCENTCOM policies and regulations.
g. Conduct STIG checks as required for new systems and at least quarterly for systems and services under USCENTCOM Authorization Official authority.
h. Produce Security Assessment Reports.
i. Support the CCR 25-28 with reviews on new and existing systems/networks.
j. Track, review, and analyze Theater Connection Approval Packages for DISN, Defense Switch Network (DSN), and Cross Domain Solutions submitted by HQ USCENTCOM, Service Components, and JTFs; ensure timely notifications are made to prevent authorization lapses (e.g., 30/60/90 day notices).
k. Provide CDS expertise; ensure CDS systems' operation is IAW applicable regulations.
l. Advise and provide recommendations to leadership on network and system risks, risk mitigation, and available COAs.
m. Develop, maintain, and execute Cybersecurity Programs and Policies.
n. Recommend network configuration, policy, training, operational, or other changes/updates based on assessed risks and/or issues IAW DoD policies and industry best practices.
o. Coordinate with internal entities, subordinate, adjacent, supporting, and senior organizations and agencies to support the resolution of security issues, authorization and connection approvals, and waiver requests.

C.5.5.3.1 CYBER POLICIES, PROGRAMS, AND INITIATIVES

The contractor shall:

a. Develop, maintain, and execute the Command Cyber Vigilance Campaign to include security training, briefs, informational papers, and pamphlets promoting cyber awareness IAW Command ISSM guidance.
b. Develop, maintain, and execute Cybersecurity Programs and Policies to include, but not limited to, CCR 380-8, the Air Gap/COMPUSEC Program, Authorized Transfer Agent / Data Transfer Officer Programs (ATA/DTO), and the Information System Security Officer (ISSO) Program IAW ISSM guidance (Section F, Deliverable 5.14).

c. In coordination with ISSM, conduct audits on Cybersecurity policies, programs and initiatives least quarterly to include DoD 8570.01-M compliance and associate workforce readiness (Section F, Deliverable 5.15).
d. In coordination with ISSM, assist the ISSM Identify, develop, audit, and initiate policy improvements as required to maintain reputational risk posture.

C.5.5.3.2 ASSESSMENT AND COMPLIANCE

The contractor shall:

a. Track and maintain authorization information databases, websites and tools to ensure that USCENTCOM networks, systems, and devices are properly documented and managed from a security perspective. These include, but are not limited to: Government Interconnection Approval Process (GIAP) database; Standard Network Access Protocol (SNAP) database; Ports, Protocols, and Services Management (PPSM); DoD IT Portfolio Repository; DoD IT SIPRNet Registry; Enterprise Mission Assurance Support Service (eMass); FISMA; DoD Cybersecurity Scorecard; local databases, sites, and systems.
b. Perform A&A of systems and networks IAW DoD policies and industry best practices.
c. Operate and maintain eMass in support of A&A activities.
d. Perform yearly ISSO control reviews in eMass for all systems currently under USCENTCOM AO authority.
e. Review, analyze, document and advise on the life cycle security requirements of applications, systems, and networks.
f. Perform system and network security assessments and policy support tasks.
g. Conduct security architecture design reviews for new systems and services to ensure compliance with defense in depth policies requirements.
h. Serve as an Operational Planning Team Member or coordinating/supporting member for operational and/or planning tasks assigned to the Cybersecurity A&A.
i. Recommend connection approval, disapproval, or modification based on security risks, DoD policies, and industrial best practices.
j. Conduct routine auditing of network and system security controls, Plans of Action and Milestones (POA&Ms), Task Order Compliance Tracking, upgrades, and new systems as required.
k. Perform network and system policy audits and configuration reviews to include reviews of Host-Based Security System (HBSS).
l. Monitor and enforce policy adherence and system configuration requirements for Program of Record (POR) systems.
m. Serve as an Operational Planning Team Member for coordinating/supporting member for operational and/or planning tasks assigned to the Cybersecurity A&A.
n. Maintain a program to monitor wireless access point and / or portable electronic devices.
o. Support Theater Connection Approval activities including:
    1. Maintaining, tracking, and validating DISN, DSN, and CDS Connection Approval Packages for USCENTCOM to include Components and JTFs.

2. Ensure timely notifications are made to prevent lapses in accreditations (e.g., 30/60/90 day notices) (Section F, Deliverable 5.16).
3. Ensure current theater networks and systems maintain authorization to operate as they are modified to meet operational requirements.
4. Review and support A&A for theater systems and networks fielded or supported by USCENTCOM staff directorates, Components, and JTFs.

p. Support Cross Domain Interoperability activities including:

1. Providing cybersecurity subject matter expertise to support the evaluation of current and emerging guard and CDS techniques, technologies, and vulnerabilities; publish reports and briefs as required.
2. Keep CDS systems current and operational on USCENTCOM networks IAW applicable regulations and maintain authorization to operate as they are modified to meet operational requirements; provide briefs as required.
3. Provide technical advice/recommendations for meeting new CDS requirements; publish a report documenting this information.
4. Attend DISN Security Accreditation Working Group or Flag Panel meetings to advocate USCENTCOM, Component, or JTF requirements.
5. Provide situational awareness of CDS systems in the USCENTCOM AOR, including location, capability, network topology/diagrams, missions supported, and other related information; publish a report to document this information on a monthly basis.
6. Manage and track requests/requirements for CDS systems supported within the USCENTCOM AOR; staff packages for prioritization and approval to the appropriate authorities; provide Phase tracking and management.
7. Review and develop Security Test and Evaluation Plans if necessary.
8. Assist USCENTCOM and Components/JTFs in meeting documentation/ processing requirements to support CDS system requests.
9. Coordinate with USCENTCOM Directorates and Components to ensure they have the proper accreditation, Secret and Below Interoperability (SABI), and connection approval documentation. Ensure timely notifications are made to customers to prevent lapses in the CDS accreditations Defense System Acquisition Working Group (DSAWG) approval process (e.g., Phases I – IV).

C.5.5.3.3 VULNERABILITY AUDIT AND ASSESSMENT

The contractor shall:

a. Maintain and operate Assured Compliance Assessment Solution (ACAS).
b. Perform vulnerability assessment scans of all internal networks, systems and applications under USCENTCOM AO authority.
c. Track and report compliance; maintain vulnerability tracking and mitigation trends (Section F, Deliverable 5.17).
d. Provide vulnerability investigation as required to assist vulnerability mitigation.

e. Provide vulnerability assessment reports as required (Section F, Deliverable 5.18).
f. Perform network discoveries and maintain network topologies in order to trend network changes over time.
g. Interface and provide support for maintaining the Continuous Monitoring Risk Scoring (CMRS) system.

C.5.5.4 SUBTASK 4 - SECURITY AND POLICY REVIEW

The contractor shall coordinate the command-wide assessment of DoD Prepublication Security Reviews (DOPSR) in order to minimize the likelihood of an inadvertent disclosure of classified or sensitive information to the public IAW DoD Directive 5230.09, Clearance of DoD Information for Public Release and DoD Instruction 5230.29, Security and Policy Review of DoD Information for Public Release. This shall include a complete assessment and thorough review of the material requested for review through the official DOPSR process.

The contractor shall:

a. Document, maintain, and communicate the most thorough and effective process for the review of DOPSR manuscripts.
b. Distribute materials to personnel assigned from command-wide, cross-functional areas (including sub-components).
c. Collect and manage inputs from intelligence, operations, communications, strategy, plans and policy, and public affairs staffs, at a minimum.
d. Provide Cybersecurity subject matter expertise to support the evaluation of existing IT platforms, critical Command and Control (C2) applications or vulnerabilities that have the potential, if publicly disclosed, to impact operations.
e. Track and report status.
f. Provide risk assessment reports, as required, to aid in supporting public disclosure recommendations.
g. Consolidate input and staff an official response for Chief of Staff signature, along with recommendations and/or reasoning for any public release limitations.
h. Coordinate and deliver timely responses to the Defense Office of Publication and Security Review.

C.5.6 TASK AREA 6 – OFFICE OF THE CHIEF INFORMATION OFFICE (OCIO) SUPPORT

C.5.6.1 SUBTASK 1 – STRATEGY AND GOVERNANCE

The OCIO (CCJ6-DCIO) supports and executes the authorities, functions, and responsibilities of the USCENTCOM Chief Information Officer (CIO). Under direction of the Deputy CIO (DCIO), the OCIO sets overall strategy and policy to govern and optimize the USCENTCOM Coalition, Command, Control, Communications and Computer System (C5) capabilities and to assure effective, secure, and efficient command IT are compliant with applicable DoD and Chairman, Joint Chiefs of Staff (CJCS) regulations and directives regarding IT resource management.

The contractor shall:

a. Advise the CIO regarding a network-enabled enterprise approach to C5 Enterprise and IT application within the Command to ensure USCENTCOM's compliance with applicable legislative, DoD, and CJCS regulations and directives.
b. Coordinate CIO policy objectives and initiatives with USCENTCOM C5 Enterprise activities (Section F, Deliverable 6.2).
c. Research, analyze, and review legislative, DoD, OSD, and JS guidance, publications, and policies and provide recommendations to the CIO.
d. Create staff packages and provide documentation including, but not limited to, white papers, information papers, decision papers, point papers, PowerPoint presentations, spreadsheets, databases, webpage design, training and education packages, policy, and guidance IAW USCENTCOM regulations, standards, and processes to facilitate the CIO objectives and intent.
e. Review the USCENTCOM C5 Enterprise strategy and associated policies and identify gaps and inefficiencies.
f. Research and develop key objectives, policy, and governance, for enterprise management of Command Information Resources in accordance with the requirements established by the Clinger-Cohen Act 1996, Information Technology Management Reform Act, 1996 and other applicable DoD, JS, and USCENTCOM directives in order to identify potential gains in effectiveness and efficiencies.
g. Review and support development of USCENTCOM C5 Enterprise strategies and priorities, including Command goals for enabling the warfighter and decision makers through the effective application and alignment of IT.
h. Coordinate, track, and manage the Command IT capability requests, per USCENTCOM regulation 25-28 processes.
i. Facilitate Command visibility of IT expenditures within its IT portfolios in accordance with CCR 25-28.
j. Coordinate, track, and assess compliance with USCENTCOM CIO policy and procedures. When necessary, report non-compliance and recommend actions to address any such non-compliance.
k. Research, recommend, and develop documentation to support CIO Governance of the Command C5 Enterprise and associated IT Management concepts.
l. Attend working groups, meetings, and conferences to include stateside, overseas, and USCENTCOM's AOR. This also includes membership of the Director's Strategy Group (DSG).
m. Coordinate, prepare, and execute the activities of USCENTCOM CIO-directed Working Groups and Boards. This includes developing the charter, preparing the agenda, managing the information in support of the agenda, preparing read-a-heads, and publishing minutes from each session.
n. Coordinate, review, analyze, and draft responses to DoD, OSD, JS, USCENTCOM, and Directorate tasks IAW USCENTCOM staffing procedures and guidance.
o. Implement the J6 Information Resource Management strategy.

p. Draft USCENTCOM theater policy and guidance to govern the use of program area applications, systems, and IT capabilities (Section F, Deliverable 6.3).
q. Represent and participate in Boards, Bureaus, Centers, Cells, and Working Groups (B2C2WG) as necessary to communicate CIO positions and acquire information.
r. In support of these activities, develop, write and or produce staff products as required (Documents, spreadsheets, presentations, etc.).

C.5.6.2 SUBTASK 2 – STRATEGIC ANALYSIS AND TASKER MANAGEMENT

The contractor shall provide strategic analysis of IT issues and priorities for DoD, Combatant Commands (CCMDs), Services and Agencies. This includes researching C5 capabilities, IT products, and reviewing command positions relative to C5 issues now and in the future. The contractor shall manage internal and external tasks for CCJ6/CIO and ensure they are assigned to the respective Divisions with relative equities.

The contractor shall:

a. Develop, recommend, and advance USCENTCOM CCJ6/CIO positions through formal review and evaluation of Strategic and Operational documents.
b. Prepare Command responses to JS or OSD regarding C5 Tasks, associated analyses, and documents assigned to the J6/CIO.
c. Prepare supporting documentation for J6 staff to participate and represent command positions on key issues at strategic DoD conferences, working groups, boards, and forums to include Functional Capabilities Board (FCB), Integrated Priority List (IPL) conferences, etc.
d. Manage the J6/CIO Joint Mission-Essential Task List and Sub-Tasks, to include maintaining input to Defense Readiness Reporting System (DRRS).
e. Perform research and data collection in support of associated Strategic, Joint Capability Integration Document System (JCIDS), and Solution Architecture tasks.
f. Develop briefings, position papers, and other supporting staff artifacts (Section F, Deliverable 6.2).
g. Coordinate with the CDR and Staff to represent USCENTCOM requirements at C4/Cyber Functional Capability Boards.
h. Coordinate J6 Capability Gap Analysis (CGA) activities and support the development of the J6 contribution to the Command's IPL.
i. Manage J6 Staff Actions with the Task Management Tool (TMT).

C.5.6.3 SUBTASK 3 – ARCHITECTURE SUPPORT

The contractor shall support the development of the USCENTCOM Enterprise Architecture (EA). This support includes researching EA products, developing federated EA products, developing a transition plan describing how USCENTCOM will transition from the As-Is (now) to the To-Be (future) and providing solutions to recommendations on USCENTCOM EA issues for the As-Is (now) and in the To-Be (future). The USCENTCOM EA shall align to the DoD Information Enterprise Architecture (IEA), and DoD Joint Capability Area's (JCA), DoD Joint

Common Systems Function List (JCSFL), Cybersecurity Reference Architecture (CS RA), Universal Joint Task List (UJTL), USCENTCOM Mission Essential Task List (METL) and supporting processes, as well as capability evolution in support of the USCENTCOM IT Portfolio Manager and CIO. The EA shall comply with and incorporate existing and future USCENTCOM planning documents, as well as apply Government and industry best practices, and standards, and utilize the command architecture development tool/repository (Casewise) to include compliance with the DoD Architecture Framework (DoDAF) and other DoD policies, modified to appropriately reflect the USCENTCOM environment.

The contractor shall:

a. Provide subject matter expertise on Command strategies, missions, roles, functions, and theater support requirements to perform near-, mid-, and long-term enterprise and strategic C4 planning (Section F, Deliverable 6.1).
b. Research, develop, and maintain the Command Enterprise Architecture including architecture products for operational, system, and technical components (Section F, Deliverable 6.1).
c. Produce warfighter domain architectures that fully address joint/coalition mission threads (operational facilities, tasks, billets, and processes) and current and future C2, Net-Centric, Focused Logistics, Joint Training, Force Application, Force Management, Force Protection, and Battlespace Awareness capabilities.
d. Analyze USCENTCOM architectures, Warfighting, Business, Enterprise Information Environment (EIE) processes, and IT to identify mission capability gaps, overlaps, and shortfalls; identify and recommend architectural, IT, or process solutions.
e. Research and develop other EA component and architecture documents and plans.
f. Provide site survey and data collection to assist USCENTCOM EA strategic planning throughout the AOR (Section F, Deliverable 6.4).
g. Provide recommendations and technical input on JCIDS documents.
h. Identify future technology and Joint Force capabilities and potential architectural and capability impacts for USCENTCOM.
i. Provide recommendations regarding the CCJ6 Strategic Architectures Line of Effort (LoE) organization and functions.
j. Understand and use the DoDAF Meta-model Ontology. Participate in DoD EA conferences, theater/Component communications conferences, and Command, Control, Communications, Computers, Intelligences, Surveillance, and Reconnaissance (C4ISR) and Architecture Working Groups.
k. Attend DoD, JS, and Combatant Command meetings.
l. Develop and maintain effective working relationships with the USCENTCOM staff and counterparts at the Office of the Assistant Secretary of Defense (Networks and Information Integration (OASD (NII)), JS, Components, JTF’s host-nations, coalition, and other agencies.
m. Develop the CENTCOM Enterprise Architecture (CEA) with encompassing transition plan to guide USCENTCOM transition from the As-Is to the To-Be architecture - Annually (Section F, Deliverable 6.5).

n. Leverage architecture tools (currently Casewise or MagicDraw) and the MS Office Suite to produce EA products, reports, and presentations.

C.5.6.4 SUBTASK 4 – SERVICE TRANSITION

USCENTCOM is responsible for multiple networks, including U.S.-only classified and unclassified, as well as Coalition and bilateral networks. The contractor shall establish and operate a Change, Configuration and Release Management program for USCENTCOM locations that are funded, managed and/or controlled by USCENTCOM HQ. Change and Release Management will primarily focus on high risk, high impact changes to IT services and Configuration Management will focus on the items/assets required to deliver IT services. The contractor shall standardize methods, processes, and procedures to control and improve the quality of the day-to-day operational IT support. These methods, processes, and procedures will align with the latest industry best practices (e.g., ITIL "Best Practices" within Service Transition).

The contractor shall:

a. Analyze and support CCJ6 management on the development of Service Transition policies and procedures for CCJ6 approval and implementation. Develop and maintain regulations, TTP, and SOP documentation of procedures and processes of how duties are performed (Section F, Deliverable 6.8).
b. Support Change Management activities:
    1. Ensure completion of technical risk assessments prior to completion of change.
    2. Identify, manage, monitor, review, trend and record changes as they progress through the system.
    3. Ensure proper documentation/authorization for proposed changes.
    4. Support the scheduling and facilitation of the IT Change Advisory Board (CAB).
    5. Monitor and report unauthorized, rejected, cancelled, emergency and successful changes to leadership as requested.
    6. Develop and maintain standardized methods and procedures to be used for efficient and prompt handling of changes.
c. Support Configuration Management activities:
    1. Maintain and control all versions of existing Configuration Items (CIs) used in the provision and management of IT services.
    2. Monitor, track, and ensure that the software in use on USCENTCOM networks has licenses and maintenance agreements.
    3. Research licensing alternatives and present the best licensing alternatives to USCENTCOM. Consider usage trends, migration plans, operational changes, and return on investment (ROI) when researching alternatives.
    4. Maintain the approved hardware/software list for all authorized software and hardware.

5. Implement and maintain a Configuration Management Database (CMDB) that contains details of the CIs throughout their life cycle and that provides accurate information to support all the other service management processes.
6. Schedule audits against the CMDB to verify the data remains current and accurate (CMDB Reconciliation).
7. Maintain and control software contracts and renewals.
8. Develop and control a naming convention process for hardware on the operational networks.
9. Provide asset management access to the CMDB to implement a hardware maintenance/warranty program to monitor and track assets.

d. Support Release Management activities:
    1. Report failed releases and perform AAR.
    2. Oversee the successful rollout of hardware and software releases into production.
    3. Coordinate the content and schedule of the rollout plan, testing plan, and all other documentation pertinent to the release.
    4. Ensure Release Coordinators harmonize with other Release Coordinators for Release packages that span multiple operational areas.
    5. Coordinate the type of information to be recorded for the release package into the CMDB. Release Management Participate or Facilitate Service Transition Working Groups.
e. Deliver monthly status report to include Audits, performance and configuration management metrics (Section F, Deliverable 6.6).

C.5.6.5 SUBTASK 5 – INFORMATION TECHNOLOGY (IT) PORTFOLIO MANAGEMENT

USCENTCOM will meet the DoD mandate of managing IT investments as portfolios. USCENTCOM will ensure all IT systems introduced within the USCENTCOM Enterprise comply with DoD and JS requirements prior to receiving an authority to connect to USCENTCOM Enterprise networks. Contractor support shall increase the effective execution of IT Enterprise Portfolio Management policies, procedures and responsibilities to improve provisioning, operation and management of USCENTCOM IT systems, services, projects, and capabilities.

The contractor shall:

a. Guide the initiation, selection, prioritization, review and balancing of the IT project portfolio over time to ensure alignment with current strategic end states as defined in USCENTCOM strategy and architectures.
b. Ensure proper integration, synchronization, and coordination of IT Enterprise requirements within the services portfolio to balance current and planned IT investments.

c. Analyze and assess effectiveness, efficiency, compliance, and establish the means to aggregate results for common awareness, to support decision-making and facilitate continual improvement within the IT Enterprise.
d. Facilitate Command visibility of IT expenditures within its IT portfolios.
e. Provide subject matter expertise in Joint Capability Area (JCA) processes to analyze, select, control, evaluate, and terminate IT capabilities as required.
f. Conduct annual reviews of JCA IT capabilities to ensure validity with current warfighter mission requirements.
g. Coordinate, track, and manage, the Command capability requests.
h. Research, analyze, and review legislative, DoD, OSD, and JS guidance, publications, and policies and provide recommendations to the CIO.
i. Research and develop Project Management Charters.
j. Coordinate and attend all IT CAB sessions and create meeting minutes (Section F, Deliverable 6.7) and post them to the IT CAB portal.
k. Coordinate with program managers/system owners to ensure complete and accurate Government Risk and Compliance (GRC) packages are submitted; solicit support of SME (internal and external) where needed.
l. Monitor and report the status of systems within the GRC process.
m. Provide reports (desk note and Letter of Introduction) confirming IT system compliance with the GRC process.
n. Attend working groups, meetings, and conferences to include stateside, overseas, and USCENTCOM's AOR.
o. Coordinate IT systems within the GRC process with (internal and external) SMEs to ensure IT system comply with DoD and Joint Staff regulations/instructions/policy. Determining:
    I. Technical feasibility, interoperability, compatibility, supportability and functionality of new or modified IT.
    II. Cybersecurity requirements, risks, and impacts.
    III. Requirement refinement and resource impacts.
    IV. Operations and maintenance impacts.
p. Create staff packages and provide documentation including, but not limited to, white papers, information papers, decision papers, point papers, PowerPoint presentations, spreadsheets, databases, SharePoint, training packages, policy, and guidance IAW USCENTCOM regulations, standards, and processes to facilitate the CIO objectives and intent.
q. Develop and maintain USCENTCOM CIO regulations and instructions.
r. Research, analyze, and review legislative, DoD, OSD, and JS guidance, publications, and policies and provide recommendations to the CIO.
s. Prepare metrics, reports, and summaries, as required, to support (internal/external) requests for information.

t. Coordinate, audit, and oversee processing of USCENTCOM Partner Nation Cybersecurity Risk Reviews (PNCRR).

C.5.6.6 SUBTASK 6 – DOD PROGRAM OVERSIGHT

The Joint Information Environment (JIE) is a single, joint, secure, reliable and agile command, control, communications and computing enterprise information environment to which the US Central Command is transitioning. JIE will consist of networked operations centers, a consolidated set of core data centers, and a global identity management system with cloud-based applications and services. The JIE will allow the information environment to flexibly create, store, disseminate, and access data, applications, and other computing services when and where needed. The Mission Partner Environment (MPE) is a set of capabilities that enable the DoD to execute its assigned missions with external partners through timely and secure sharing of mission information.

The contractor shall:

a. Provide JIE, MPE, and Mission Partner Environment – Information System (MPE-IS) support for Integrated Process Teams (IPTs), Integrated Design Teams (IDTs), and In-Progress Review (IPRs). Attend and/or support working groups, committees, and boards.
b. Coordinate JIE, MPE, and MPE-IS actions across the USCENTCOM staff, other CCMDs, JS, and DoD CIO to facilitate compliance with policy, strategic objectives, and portfolio plans for projects.
c. Produce decision and information briefings/papers and status frameworks for all applicable programs, projects, or processes.
d. Provide management oversight to include IPRs, status updates, and coordination for all JIE, MPE, and MPE-IS-related initiatives to ensure continued situational awareness is maintained, synchronization, and planning factors/activities are executed.
e. Routinely attend and actively participate in high-level meetings, conferences, and seminars with Command leadership, JS, and interagency; provide summary of sessions and surmise relevancy to leadership.
f. Prepare read a-heads, 5x8, preparatory information/summaries of events relative to JIE, MPE, and MPE-IS events.
g. Prepare metrics, reports and summaries, as required, to support (internal/external) requests for information.
h. Monitor and report the status of ongoing projects and C5 initiatives supporting USCENTCOM to JIE and MPE.
i. Coordinate with project managers to ensure consistency in project reporting (internal and external stakeholders); solicit support of SME where needed
j. Facilitate coordination/planning sessions, working groups and IPRs, as needed, to validate/promote continued progress toward JIE and MPE transition.

C.5.7 TASK AREA 7 – RESOURCE MANAGEMENT SUPPORT

C.5.7.1 SUBTASK 1 – RECORDS MANAGEMENT

Operations Iraqi Freedom (OIF), New Dawn (OND) and Enduring Freedom (OEF) resulted in the mass migration of millions of documents back to USCENTCOM, which took over the responsibility of managing this record material at the end of a mission. OEF ended on December 31, 2014 and transitioned to Operation Freedom's Sentinel (OFS) on January 1, 2015. USCENTCOM will continue the responsibility of managing record material from current and future contingency events and named operations.

The contractor shall provide electronic records analysis and support to the Command in organizing and managing the digital collection for preservation purposes in order to meet legal obligations under the Federal Records Act. Additionally, the contractor is responsible for continual implementation of a DoD 5015.02-compliant electronic records management application (ERMA); e.g., Hewlett Packard Enterprise Content Manager (HPECM) ERMA and updated versions to the Directorates/Special Staff at both HQ USCENTCOM and CFH. The contractor shall support the ERMA/SharePoint/Task Management Tool integration as part of a greater KM Program initiated by the CCJ6/Chief of Staff.

The contractor shall provide records management support of USCENTCOM War Records migration, including work on organizing records the Command receives from past, current and future named operations, purging redundant records, migrating final records into the ERMA, and adding required metadata to documents so records are properly tagged for quicker research and retrieval.

The contractor shall:

a. Support the CCJ6-R and CCJ6-E staff on the integration of the ERMA and MS SharePoint 2010, 2013, or updated versions.
b. Support the CCJ6-RDR (Records Management Section) Section Chief in the development of information taxonomy for all USCENTCOM Records and make recommendations to the existing records taxonomical structure currently used within the ERMA.
c. Process Command records into the ERMA and report status on a monthly basis.
d. Provide training to all CCJ6-R personnel and any other USCENTCOM records staff on ERMA use.
e. Support the CCJ6-R and Secretary Joint Staff (SJS) personnel in the transfer of TMT records into the ERMA.
f. Coordinate support with ERMA and TMT vendors to continue integration between the two products.
g. Support CCJ6-R personnel with Active Navigation and eDiscovery solutions to better improve the document analysis of the USCENTCOM collections.
h. Provide a monthly status report of records migrated to HPECM (Section F, Deliverable 7.1).
i. Support troubleshooting of any ERMA-related issues and maintain records of all customer support requests (Section F, Deliverable 7.2).
j. Support the expansion of ERMA usability across USCENTCOM networks (e.g., CPN-X, JWICS). Support the CCJ6-RDR in the transfer of records to the National Archives via

the ERMA Export utility and develop an executable PDF batch conversion methodology for the Command.

k. Convert to electronic format, compatible with USCENTCOM's ERMA, physical Permanent and Long Term Temporary war-related records. Documents must be scanned to 600 Dots per Inch (DPI) and converted to Optical Character Recognition (OCR) and remain on-site.
l. Increase CCJ6-R's capabilities to search for, collect, preserve, and analyze records that are responsive to JS, Litigation and Freedom of Information Act (FOIA) requests.
m. Prepare scanned records for destruction.
n. Review all electronic records (one by one) to identify official records for inclusion in CENTCOM's ERMA.
o. Ensure all records identified in CENTCOM's ERMA are appropriate for storing to maximize the use of server/storage space.
p. Maintain metrics on length of time taken to process each assigned folder(s).

C.5.7.2 SUBTASK 2 – INVENTORY MANAGEMENT

C.5.7.2.1 USCENTCOM HQ INVENTORY MANAGEMENT

USCENTCOM requires Inventory Management Analysis support to maintain consistent accountability of IT assets supporting HQ USCENTCOM. The contractor shall assist with the operations of the HQ Project Support Facility (PSF) in accordance with the SOPs. Operations support includes, but is not limited to, shipping and receiving support of IT assets, storage of computer/communications-related assets, and distribution of hardware in conjunction with Government-delivered distribution plans at HQ in support of the AOR. The contractor shall ensure that all IT hardware and software are properly received, documented, stored, and disbursed to the required user to maintain good supply and accountability of IT. The contractor is responsible for asset inventories at the Project Support Facility and IT warehouse.

The contractor shall:

a. Conduct receiving, labeling and properly documenting all incoming equipment.
b. Perform distribution and shipping of all IT equipment at the HQ and the AOR.
c. Ensure all property items are uniquely labeled, tracked and changes inputted into the database.
d. Inspect goods and materials and assess condition for distribution/recycling.
e. Coordinate the disposal of property, supplies, and or material in compliance with Government and/or military regulations/guidelines.
f. Maintain records of acquisition/distribution and property, supplies, and materials.
g. Investigate and reconcile discrepancies.
h. Process excess IT equipment as identified by CCJ6 using CENTCOM and DoD procedures.
i. Maintain accountability and separation of CCJ6 Directorate project Bill-of-Materials.

j. Inventory PSF and IT warehouse and maintain records of materials and equipment stored in these facilities; provide monthly report (Section F, Deliverable 7.3).
k. During surge inventory processes, aid each Directorate with completing weekly, quarterly, and annual inventories.
l. Conduct asset inventory (to include Sensitive Compartmented Information Facility (SCIF) areas, e.g., Vince Bldg. 569).

C.5.7.2.2 FORWARD HQ (CFH) INVENTORY MANAGEMENT

USCENTCOM requires Inventory Management Analysis support to maintain consistent accountability of IT assets supporting HQ USCENTCOM. The contractor shall operate the CFH Inventory Management Facility in accordance with the standard operating procedures. Operations shall include, but is not limited to: conduct shipping and receiving of IT assets, storage of computer/communications-related assets, and distribution of hardware in conjunction with Government-delivered distribution plans at CFH, in support of Qatar and Kuwait. The contractor shall ensure that all IT hardware and software are properly received, documented, stored, and disbursed to the required user to maintain good supply and accountability of IT equipment. The contractor is responsible for asset inventories at CFH, and Camp Arifjan - Kuwait.

The contractor shall:

a. Schedule and revise shipment plans to ensure efficient distribution of products to satisfy customers.
b. Analyze inventory levels, production speed, and product demand to determine reorder levels, which shall ensure product availability and minimize inventory costs.
c. Manage inventory levels to efficiently utilize capital investment while maintaining adequate coverage for known/projected demand.
d. Maintain control and accountability over assigned products; determine appropriate distribution based on lead times and demand.
e. Handle the acquisition of property, supplies, and/or materials from other agencies, to include transporting and storage.
f. Ensure all property items are uniquely identified and changes are tracked and recorded.
g. Inspect goods and materials and assess condition for distribution/recycling.
h. Coordinate the disposal of property, supplies, and or material in compliance with Government and/or military regulations/guidelines.
i. Maintain records of acquisition/distribution and property, supplies, and materials.
j. Investigate and reconcile discrepancies.
k. Process computer assets to/from the SCOs in the AOR when equipment is going from CFH.
l. Process excess IT equipment as identified by CCJ6 using DoD procedures.
m. Maintain accountability and separation of CCJ6 Directorate project Bill-of-Materials.
n. Conduct weekly, quarterly and annual inventories; provide report quarterly and annual roll-up (Section F, Deliverable 7.3).

o. Research and reconcile any inventory discrepancies.

C.5.8 TASK AREA 8 – KNOWLEDGE MANAGEMENT (KM)

The USCENTCOM Knowledge Management (KM) office is responsible for management and operations of the enterprise-wide KM Program. The KM program develops, maintains, and integrates KM resources and activities throughout HQ USCENTCOM and the Components. The KM Program develops and integrates tools to support command and staff processes, activities, and tasks, and provides training and awareness of KM resources throughout USCENTCOM. The contractor shall assist in supporting USCENTCOM in operating, monitoring, managing, maintaining, and developing the KM Program. During continuity of operations, at least some of the KM team is expected to continue the program from alternative sites, including USCENTCOM CFH, Al Udeid AB, Qatar. The contractor may be required to support the relocation efforts associated with these objectives. Additionally, the KM collaboration tools used in processes reside on JWICS, SIPRNet, NIPRNet, and coalition networks.

C.5.8.1 SUBTASK 1 – PROGRAM AND PROJECT MANAGEMENT

The contractor shall:

a. Provide development, maintenance, and improvement of USCENTCOM's KM Program to include goals, objectives, mission, vision, and implementation plans in a KM strategy product (Section F, Deliverable 8.1).
b. Provide preparation and development of KM Project Plans; this may include, but is not limited to, preparing information papers/reports and presentations on KM projects (Section F, Deliverable 8.2).
c. Provide development, monitoring, and execution of any KM assessment programs or studies.
d. Advise and assist in the development, monitoring, and execution of any KM assessment programs or studies.
e. Provide project management expertise on KM initiatives within USCENTCOM; this includes, but is not limited to, monitoring the KM programs and/or projects and providing recommendations to integrate cross-directorate KM projects.
f. Provide requirements gathering, analysis, and recommendations of IT requirements change process when determined to be appropriate (Section F, Deliverables 8.3 and 8.4).
g. Develop a marketing campaign to ensure USCENTCOM headquarters personnel are familiar with collaboration applications and familiar with tools and resources for maximum awareness and effective employment of the applications and tools.
h. Conduct detailed analysis and identification of operational processes and procedures, and provide recommendations and process map (Section F, Deliverable 8.5).
i. Identify and document processes that could be handled by capabilities and features within the Command's collaboration tools, to include SharePoint portals.
j. Engage stakeholder community to ensure successful implementation and sustainment of KM processes and procedures.

k. Interface regularly with USCENTCOM and Component KM personnel and those related to KM.

l. When KM is hosting meetings, expect to coordinate inputs, products and/or briefs, ensure attendees are invited with sufficient time for reasonable attendance; read a-heads are reviewed, approved, and sent to attendees at least 24 hours prior to KM meeting or 72 hours for meetings with Commander, Deputy Commander, or Chief of Staff. The contractor shall capture, track, analyze, and compare attendance and provide minutes and track actions.

m. Document and capture KM processes and procedures (SOPs) (Section F, Deliverable 8.6).

n. For Command processes, be prepared to assist staff to develop and document process maps and information flow models.

o. Expect tasking through the task management system to review KM and non-KM policies, procedures, doctrine, directives, manuals, instructions, and manuscripts.

p. Routinely attend, present, and actively participate in high-level meetings, conferences, and seminars with Command leadership, JS, and interagency to advocate KM processes and programs in support of HQ USCENTCOM, Component Commands, and deployed JTFs.

q. Consolidate and provide KM comments for recurring, required activity reports for review and approval (Section F, Deliverable 8.7).

r. Consolidate and provide quarterly KM history reports for review and approval (Section F, Deliverable 8.8).

s. Develop customer feedback process, document feedback, and recommend and implement changes to improve customer satisfaction (Section F, Deliverable 8.9).

C.5.8.2 SUBTASK 2 – EXERCISES AND OPERATIONS

The contractor shall:

a. Develop, maintain, and implement the USCENTCOM KM plan corresponding to the USCENTCOM Theater Campaign Plan for day-to-day theater objectives, activities and operations. (Section F, Deliverable 8.10)

b. Develop, maintain, and implement KM plans for Operation Plan (OPLAN), Concept Plan (CONPLAN), and Operation Orders (OPORDs) to describe KM in unique mission command and control organizations, mission partners, and/or unique communications capabilities (or limitations). Ensure the plans and implementations are integrated with data/information management guidance, the Original Classification Authority's (OCA's) Security Classification Guidance, and OPSEC guidance (Section F, Deliverable 8.11).

c. Develop, maintain and implement KM plans for command exercises as determined appropriate that describe KM for unique mission command and control organizations, mission partners, and/or unique communications capabilities (or limitations). Ensure the plan and implementation is integrated with data/information management guidance, the OCA's OPSEC guidance (Section F, Deliverable 8.12).

d. Support the development and maintenance of the command's battle rhythm event standards, templates, and governance.
e. Develop and maintain framework to assess KM readiness supporting ongoing command and staff functions for steady state and Theater Campaign Plan as well as OPLANS, CONPLANS, OPORDS, and staff exercises (Section F, Deliverable 8.13).
f. Using KM Assessment Framework, perform assessment of KM ability to support USCENTCOM steady state functions and activities, to include HQ staff and at least one Component.
g. Using KM Assessment Framework, perform assessment of KM readiness to support future USCENTCOM plans, to include at least one component.
h. Using KM Assessment Framework, perform assessment of KM readiness to support exercise execution for which USCENTCOM HQ is a training audience.
i. Manage and maintain the process, roles, and responsibilities and readiness to migrate classified plans and associated data to another network for wider dissemination. Provide a readiness status report (Section F, Deliverable 8.14).
j. Coordinate collection of KM observations, lessons learned, and best practices to be captured in the USCENTCOM's Lessons Learned Program managed by Training and Exercises Directorate (CCJ7), Directorate for Exercises and Training.
k. Establish relationships with KM teams from organizations whose commanders have direct lines of authority to Commander, USCENTCOM, to include service components and Commander, Joint Task Forces, or sub-unified commands as stakeholders to develop and implement KM plans.
l. Manage and coordinate Joint Knowledge and Information Management Working Groups (JKIMWGs).

C.5.8.3 SUBTASK 3 – TRAINING PROGRAM

The contractor shall:

a. Develop, review, and maintain training objectives for the KM module in Newcomer Orientation – a course of instruction for all USCENTCOM newcomers, managed by CCJ7 (Section F, Deliverable 8.15).
b. Deliver in classroom environment course of instruction during the weekly KM module for Newcomer Orientation. Ensure newcomer training products are consistent and ensure alternate instructor can provide the same level of training and instruction.
c. Review Newcomer Orientation feedback collected by CCJ7 to determine if and how KM module can be improved.
d. In coordination with Information Management (IM) personnel, develop and provide recurring KM educational course training objectives and curriculum for the USCENTCOM staff (Section F, Deliverable 8.16).
e. Manage and maintain the course briefs and products so that they are current, accurate, and complete.

f. For KM courses, manage scheduling, room scheduling, announcement, and registration on at least a monthly basis.
g. Deliver KM courses in classroom environments.
h. Develop and maintain Computer-Based Training (CBT) for all KM courses.
i. Develop and deliver semi-annual training report that addresses effectiveness and correlates to staff performance (Section F, Deliverable 8.17).
j. Track attendance at courses by individual and organization to be able to show how many people that are currently assigned to USCENTCOM have attended the courses. Include in semi-annual report to client.
k. Develop student feedback mechanisms for in-class and computer-based training, collect the feedback, analyze, and apply improvement to future courses. Provide semi-annual report to client.
l. Provide KM application training for implementation and sustainment. Example includes the command schedule and synchronization tool where the information provided by contributors is viewed at the highest levels. This tool is called CD-TEMPO.
m. Deliver ad-hoc training. To the maximum extent possible train in groups, but one-on-one, and deskside training may be required at times. Capture and include in semi-annual training report.

C.5.8.4 SUBTASK 4 – COLLABORATION, INTEGRATION, AND EMPLOYMENT

The contractor shall:

a. Develop plans and recommendations on how to better utilize existing information systems and collaboration tools that may be provided by USCENTCOM or enterprise tools provided by DISA, Defense Intelligence Agency or others (Section F, Deliverable 8.18).
b. Provide and maintain USCENTCOM taxonomy for SIPR and NIPR SharePoint environments and All Partner Access Network (APAN) taxonomy for USCENTCOM-managed groups and sites. For USCENTCOM purposes, taxonomy is the SharePoint hierarchy products and similar products for APAN groups and sites (Section F, Deliverable 8.19).
c. Include recommendations on the management and design of portal site collections and sites to enhance the USCENTCOM KM Program.
d. Provide recommendations and assistance in the development of innovation and technology plans that supports the USCENTCOM mission and KM goals.
e. Provide key inputs to command strategy and policy development to successfully transform HQ USCENTCOM into a learning organization that is flexible, agile, and receptive to change.
f. Remain abreast of new DoD technologies and processes in the data analysis, production, and dissemination arena in order to constantly improve, plan, and coordinate their migration into the USCENTCOM KM architecture.

g. Provide guidance for the design and conduct of comprehensive studies, to determine effectiveness of operations, flow of information, and effectiveness of KM systems across all levels of the Command.
h. Conduct research in the areas of KM, process improvement, technology, and/or organizational learning to increase the knowledge base of HQ USCENTCOM; provide improved tools and methodologies to enable the HQ USCENTCOM staff, Component Commands, JTFs, and external partners and agencies in a collaborative environment.
i. Develop critical information processing tool requirements and techniques to enhance and empower the implementation of HQ USCENTCOM KM initiatives.
j. Prepare written materials on request such as USCENTCOM Commander, Deputy Commander, and Chief of Staff Memorandums and directives, as well as other brochures, CDs, and web-based content that direct and optimize KM processes within the Command.
k. Manage USCENTCOM communities and sub-communities on APAN to support unclassified information sharing requirements within or related to USCENTCOM, the theater, missions, and objectives or supporting tasks. APAN environment includes groups and subgroups for Telligent platform and sites and subsites for SharePoint platform. Advise and train USCENTCOM (theater-wide) users on the features of APAN and what fits their needs best as well as permissions/access management.

C.5.9 TASK AREA 9 – SURGE SUPPORT

The contractor shall provide support for unanticipated, as-needed requirements that fall within the scope of the task areas (1 through 8). Examples of Extended Work Week (EWW) / surge requirements include, but are not limited to, augmenting high-level CND initiatives to battle cyber-attacks on the USCENTCOM and related networks, USCENTCOM Commander and the C4 Systems Director initiatives and exercises to improve and streamline the IT enterprise, and augmentation of the existing force in addressing communications and IT projects in the USCENTCOM AOR. The surge occurrences will be of a limited duration based on individual circumstances.

This surge support may require the use of outside, corporate ‘reach-back’ support to fix urgent issues in the course of a day to projects lasting several months. The contractor shall provide emergency technical support worldwide on short notice (e.g., two workdays). It is anticipated that a typical team may include contractor personnel for a specified period of time to provide support for urgent requirements.

The contractor shall also be available 24 hours a day, 7 days a week “on-call” support. The contractor shall adhere to a robust industry standard for “on-call” support to include appropriate response times for solving problems based on mission criticality and priority as determined by the Government.

The contractor shall not provide technical support outside the scope of this TO and shall only use the labor categories within the Alliant base contract. The use of higher skilled personnel to perform these duties shall be approved by the Government before incurrence.